Rede von Philipp Weltzien 16.3.2022 (Plenarprotokoll 7/74)

IT-Sicherheit in Thüringen gewährleisten

Aktuelle Stunde auf Antrag der Fraktion BÜNDNIS 90/DIE GRÜNEN - Drucksache 7/5046

Sehr geehrte Frau Präsidentin, sehr geehrte Damen und Herren Abgeordnete, liebe Zuschauer am Livestream! Als die Grünen letzte Woche das Thema zur Aktuellen Stunde „IT-Sicherheit in Thüringen gewährleisten“ eingereicht haben, war ihnen wahrscheinlich noch gar nicht bewusst, wie aktuell diese Aktuelle Stunde heute sein kann. Aktueller geht es kaum, denn erst letzte Woche Donnerstag wurde bekannt, dass die Stadt Suhl Ziel eines Hackerangriffs geworden ist und seitdem im Grunde genommen keinen Zugriff mehr auf ihre digitalen Daten und Systeme hat und dieser auch bis dato noch nicht wiederhergestellt werden konnte. Unter großem Aufwand ist es der Stadtverwaltung zwar gelungen, zumindest die dringenden Zahlungen an Leistungsempfänger aus dem Sozialamt pünktlich zu leisten, aber de facto – und davon habe ich mich die Woche selbst überzeugt – ist diese Stadtverwaltung weitestgehend arbeitsunfähig. Nach den Erfahrungen anderer vergleichbarer Verwaltungen wie beispielsweise in Anhalt-Bitterfeld, die auch Opfer von solchen Attacken gewesen sind, wird es auch mindestens noch ein halbes Jahr in Anspruch nehmen, bis man überhaupt wieder von Arbeitsfähigkeit sprechen kann.

Nach Angaben des Cyber-Sicherheitsrats in Deutschland haben in den vergangenen Monaten und auch in den letzten Wochen die Hackerangriffe auf Kommunen stark zugenommen. Auch vor dem Hintergrund des Angriffskriegs von Russland auf die Ukraine steigt die Gefahr eines hybriden Kriegs, also eines wachsenden Risikos unter anderem russischer Cyberattacken. Deutschland könnte es in einem noch nicht geahnten Ausmaß treffen. Aktuell werden vor allem die Bombeneinschläge des Kremls und die Annäherung an bestimmte Außengrenzen thematisiert. Fakt ist jedoch, die meisten Thüringer Unternehmen, Kommunen und Verwaltungen verfügen über eine direkte Außengrenze zu Russland und auch zu anderen Staaten, nämlich über ihre digitale Anbindung an das Internet. Soll heißen: Auch wenn sich die russischen Außengrenzen des Kriegs geografisch vergleichsweise weit weg anfühlen, kann dieser Krieg digital bereits vor unserer Haustür stehen.

Je nach Schutzniveau sind Städte und Kommunen verwundbar, sowohl gegenüber Geheimdiensten anderer Länder als auch krimineller Hacker/-innen. So konnten wir zum Beispiel exemplarisch im Dezember 2015 beobachten, wozu russische Cyberangriffe in der Lage sind. 230.000 Menschen in der Westukraine hatten keinen Zugang zu Strom, und das ist kein abstraktes Szenario aus einem Science-Fiction-Film, sondern ein Blackout, der uns treffen und sehr viel Schaden anrichten kann. In vielen Fällen ist es schwer festzustellen, wer hinter solchen Angriffen steckt. Unsere kritische Infrastruktur, insbesondere die Bereiche Energie, Telekommunikation, Krankenhäuser, Wasser und Verwaltung, ist seit Jahren abstrakt gefährdet und das Risiko ist seit Jahren bekannt. Wie der Kollege Müller bereits richtig ausgeführt hat, herrscht jedoch bundesweit ein Flickenteppich von Zuständigkeiten und Insellösungen. Im März 2021 fanden Anhörungen zum Gesetzentwurf der Bundesregierung für mehr Sicherheit in der Informationstechnologie statt. Die Anzuhörenden dort begrüßten das Vorhaben eines IT-Sicherheitsgesetzes 2.0, befanden es aber in der vorliegenden Fassung für völlig

ungenügend. Die IT-Expertinnen und -Experten vom Chaos Computer Club forderten daraufhin, Sicherheit gestalten, statt Unsicherheit verwalten. Die anstehenden Herausforderungen werden nicht angegangen, weil einfach nicht kompromisslos für IT-Sicherheit eingetreten wurde. Die Arbeitsgemeinschaft Kritische Infrastrukturen, die vorhin auch schon angesprochen wurde, fordert die Einführung eines Cyberhilfswerks. Wer sich ein Bild von der Flüchtlingssituation vor Ort gemacht hat, weiß, wie ein THW funktioniert. Gleiches muss in Krisensituationen eben auch auf der Cyberebene funktionieren, nämlich dann zum Beispiel, wenn Kommunalverwaltungen Opfer von Ransomware-Attacken geworden sind oder eben auch Schulen oder Krankenhäuser. In Deutschland gibt es aktuell nämlich fast 2.000 kritische Infrastrukturen. Demgegenüber stehen aber eben nur 15 hauptamtliche Mitarbeiter/-innen des BSI in einem solchen ähnlichen Team. Das ist eben nur mit wenig oder mit viel Aufwand um ein niedriges Vielfaches in einer geringen Zahl aufstockbar.

Diesen Forderungen können wir uns so als Linke anschließen. Wir brauchen dringend ein thüringenweites CHW und eine zentrale IT-Supportstruktur für alle Behörden des Landes und auch der Kommunen und müssen diese personell leistungsfähig ausstatten, um in Schadensfällen angemessen reagieren zu können. Zu empfehlen ist auch eine Nachbesserung in den folgenden Haushalten, um eine bessere Ausstattung in den Bereichen Cybercrime und IT-Kriminalität im LKA und Polizeiinspektionen zu gewährleisten. Offene Sicherheitslücken verursachen Schwachstellen und kennen kein Gut oder Böse. Sie sind als offene Scheunentore von Kriminellen aller Couleur gleichermaßen nutzbar und damit ein Sicherheitsrisiko für alle. Vielen Dank.

(Beifall DIE LINKE)