Landtag Brandenburg **Drucksache 7/6215-B**
7. Wahlperiode

Beschluss
des Landtages Brandenburg

IT-Sicherheit in Brandenburg stärken

Der Landtag Brandenburg hat in seiner 74. Sitzung am 13. Oktober 2022 zum TOP 4 folgenden Beschluss gefasst:

„Der Landtag stellt fest:

Die Digitalisierung hat unsere Gesellschaft und unseren Staat bereits maßgeblich geprägt. Dieser Prozess dauert an. Mit der fortschreitenden Digitalisierung sind dabei auch neue Gefahren offenbar geworden. So hat es in der Vergangenheit bereits Angriffe auf die IT-Infrastruktur des Deutschen Bundestags, auf das Datennetz des Bundes und der Sicherheitsbehörden gegeben.

In jüngster Vergangenheit musste erstmals aufgrund eines Cyberangriffs der Katastrophenfall in einem deutschen Landkreis ausgerufen werden. Auch in Brandenburg gab es bereits Vorfälle mit erheblichen Beeinträchtigungen für Bürgerinnen und Bürger.

In all diesen Fällen kam es zu kurz- oder mittelfristigen Einschränkungen oder Unterbrechungen der Verfügbarkeit staatlicher Leistungen.

Im Zusammenhang mit dem Krieg in der Ukraine hat die abstrakte Bedrohungslage im Bereich der IT-Sicherheit zuletzt stark zugenommen.

Verschiedene gesetzliche Regelungen wie die Datenschutzgrundverordnung auf Europäischer Ebene, das Bundesdatenschutzgesetz und das Brandenburgische Datenschutzgesetz (BbgDSG) sowie das in Brandenburg in der Landesverfassung verankerte Recht auf Schutz der persönlichen Daten entfalten ihre Wirkung auch hinsichtlich einer Stärkung der Informationssicherheit und sind auch mit Blick auf die fortschreitende Digitalisierung novelliert worden. Darüber hinaus gibt es eine Reihe von Rechtsgrundlagen, die mit Blick auf die Informationssicherheit neu geschaffen bzw. fortgeschrieben worden sind wie das IT-Sicherheitsgesetz 2.0 als auch das Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz - BSIG).

So wie die Digitalisierung auf allen staatlichen Ebenen vollzogen wird, so muss auch die IT-Sicherheit als Gemeinschaftsaufgabe aller Ebenen begriffen werden, um abgestimmt und erfolgreich sein zu können.

Seit dem Jahr 2011 besteht eine zwischen dem Bund und den Ländern geeinte Differenzierung der Infrastrukturen in neun Sektoren. Während für die meisten Sektoren einheitliche gesetzliche Regelungen geschaffen werden konnten, gibt es diese Einheitlichkeit im vom Föderalismus geprägten Sektor Staat und Verwaltung nicht.

So bestehen mit dem Gesetz über das Bundesamt für Sicherheit in der Informationstechnik einheitliche Kriterien und Schutzziele für den Betrieb Kritischer Infrastrukturen, nicht jedoch für die Sektoren Staat und Verwaltung sowie Kultur und Medien.

Die Landesregierung ist in diesem Bereich seit vielen Jahren etwa in der Bund-Länder-Arbeitsgruppe Kritische Infrastruktur (AG KOST KRITIS) aktiv und hat jüngst eine eigene Koordinierungsstelle Kritische Infrastruktur eingerichtet.

Auf Ebene der Länder und insbesondere der Kommunen bestehen unterschiedliche Voraussetzungen, um IT-Sicherheit zu gewährleisten. Die Einrichtung des Zweckverbandes Digitale Kommunen in Brandenburg (DIKOM), in dem sich seit seiner Gründung mehr als 50 Kommunen zusammengeschlossen haben, zeigt einen erfolgreich eingeschlagenen Weg auf kommunaler Ebene, zu dem auch das Land bereits einen Beitrag auch aus Haushaltsmitteln geleistet hat.

Es sind weitere Anstrengungen notwendig, um den bestehenden und steigenden Anforderungen in diesem Bereich in einem strukturellen, rechtlichen und technischen Rahmen zu begegnen. Mit zunehmender Digitalisierung steigt dabei auch die Dringlichkeit der Gewährleistung von IT-Sicherheit.

Der Landtag fordert die Landesregierung im Rahmen der personellen und finanziellen Gegebenheiten auf,

1. die Notwendigkeit der personellen und finanziellen Stärkung im Bereich der IT-Sicherheit, des Infrastruktur-Betriebs und bei der Einhaltung und Durchsetzung bestehender Rechtsvorschriften wie dem BbgEGovG, BSIG und der Datenschutz-Grundverordnung fortlaufend für die Landesebene zu prüfen und ein regelmäßiges Lagebild zum Stand der IT-Sicherheit sowie der personellen und finanziellen Ressourcen in diesem Bereich zu erstellen;

2. für den Sektor Staat und Verwaltung weiter an der Definition und Implementierung von Sicherheitsstandards zu arbeiten, die zur Vermeidung von Störungen der Verfügbarkeit, Integrität und Vertraulichkeit informationstechnischer Systeme beitragen. Wo möglich soll dies im Benehmen mit den anderen Ländern, dem Bundesamt für Sicherheit in der Informationstechnik und dem Bundesamt für Bevölkerungsschutz und Katastrophenhilfe geschehen. In einem ersten Schritt ist zu definieren, welche staatlichen Leistungen auf Landesebene Bestandteil der Kritischen Infrastruktur sind und diese in einem geeigneten Business Continuity Management System (BCMS, entsprechend BSI-Standard 200-4) abzubilden;

3. einheitliche und verbindliche Standards bei der Softwarebeschaffung und Softwareentwicklung in der Landesregierung zu etablieren und Ausschreibungskriterien für Software hinsichtlich der Sicherstellung von Wartbarkeit, Datenschutz und Verschlüsselung auf dem Stand der Technik sowie der digitalen Souveränität festzuschreiben;

4. zu prüfen, wie ein landesweit verbindliches Verfahren zum Umgang mit Sicherheitslücken, insbesondere im Landesverwaltungsnetz, zu erarbeiten ist, das auch verbindliche Meldeverfahren sowie Vorgaben zum Umgang mit Hinweisen aus der Bevölkerung beinhaltet;

5. zu prüfen, ob und gegebenenfalls welche weitere Unterstützung das Land den Kommunen im Bereich der IT-Sicherheit über bestehende Leistungen hinaus gewähren kann, etwa über CERT-Dienste;

6. die Perspektive und Position der Kommunen weiterhin in die Gremienarbeit einzubeziehen.“

Prof. Dr. Ulrike Liedtke
Die Präsidentin