Rede von Marie Schäffer zu: Antrag "IT-Sicherheit in Brandenburg stärken" (TOP 4 der 74. Plenarsitzung)

# IT-Sicherheit in Brandenburg stärken

*- Es gilt das gesprochene Wort!*

Sehr geehrte Frau Präsidentin, Liebe Kolleg*innen, liebe Gäste,

stellen Sie sich einmal vor, alle Computer, die in Brandenburger Behörden stehen, würden auf einen Schlag verschwinden. Jenseits von allen berechtigten Witzeleien darüber, wie weit wir in Deutschland bei der Digitalisierung hinterherhinken, ist glaube ich bei diesem Bild jedem sofort klar, was das bedeuten würde. Die Arbeit müsste quasi eingestellt werden. Selbst, wenn man manches mit Papier und Stift improvisieren könnte: spätestens an allen Stellen, wo es darum geht, Gelder auszuzahlen oder einzunehmen, kann man sich die Katastrophe gut ausmalen.

Meine Damen und Herren, leider braucht es für das eben beschriebene Szenario gar nicht so viel Phantasie. Denn dass in einer Behörde die IT plötzlich für längere Zeit unbenutzbar ist, mussten wir in Deutschland leider schon mehrfach erfahren. Besondere Aufmerksamkeit erhielt der Landkreis Anhalt-Bitterfeld, wo im Juli 2021 sogar der Katastrophenfall ausgerufen werden musste, nachdem ein Erpressungstrojaner, sogenannte Ransomware, die dortige IT-Infrastruktur komplett lahmgelegt hat. Das Ergebnis sind etwa 2.000.000 € entstandene Kosten, ein mehr als einjähriger Wiederaufbau der IT-Infrastruktur mit großen Betriebseinschränkungen, teilweise unwiederbringlich verlorene Daten, und nicht zuletzt ein großer Vertrauensverlust in den Staat.[1]

Auch in Brandenburg hatten wir schon ähnliche Vorfälle, wenn auch von etwas kleinerem Ausmaß. In Potsdam mussten im Januar 2020 nach einem festgestellten Angriff auf die Software Citrix alle Systeme heruntergefahren werden. Allein das sichere Neustarten der

Infrastruktur hat über ein Jahr gedauert und hat zehntausende Euro an Kosten verursacht[2].

Etwas, was diese und viele andere Vorfälle gemeinsam haben, ist, dass sie nach aktuellen Kenntnisstand von heutzutage leider ganz gewöhnlicher Internetkriminalität ausgelöst wurden. International agierende Gruppen haben ein höchst lukratives Geschäftsmodell daraus entwickelt, Netze von Unternehmen und Behörden zu infiltrieren, Daten zu verschlüsseln oder auszuleiten, um dann Lösegeld dafür zu fordern, die Daten nicht zu löschen oder zu veröffentlichen. Das sind keine einzelnen Vorfälle, sondern es ist ein Massenphänomen, das unserer Wirtschaft jedes Jahr unermessliche Schäden zufügt. Hier ist dringender Handlungsbedarf in der Politik und ich freue mich, dass auf Bundesebene darüber intensiv diskutiert wird, wie wir unsere Wirtschaft bei der Absicherung ihrer Infrastruktur unterstützen können.

Aber: Diese Art der Kriminalität ist eher ein Grundrauschen in einem weltweiten Netz, für das absehbar kein effektiver internationaler Rechtsrahmen zur Verhinderung und Verfolgung solcher Straftaten existieren wird. Dass immer wieder auch kritische Infrastrukturen in Deutschland davon betroffen sind, zeigt, wie viel Arbeit noch vor uns liegt.

Denn von unseren unverzichtbaren staatlichen Infrastrukturen müssen wir erwarten können, dass sie nicht nur gegen solche gewöhnlichen Gefahren gewappnet sind, sondern auch, dass sie resilient sind gegen ernsthafte Angriffe staatlicher oder staatlich unterstützter Akteur*innen.

In Deutschland haben wir viel zu lange mit den Schultern gezuckt und darauf vertraut, dass sich schon niemand dafür interessieren würde, unsere Infrastruktur anzugreifen. Und das während seit vielen Jahren immer offensichtlicher wird, dass verschiedenste skrupellose Akteur*innen bewusst internationale Konflikte durch offene oder klandestine Cyberangriffe erweitern.

Nach dem Angriffskrieg Russlands auf die Ukraine und den damit verbundenen digitalen Angriffen muss mit dieser Haltung endgültig Schluss sein. Wir müssen uns klarwerden,

dass wir uns eine derartige Verwundbarkeit unserer kritischen Infrastruktur nicht leisten können – weder im physikalischen noch im virtuellen Raum. Der Schaden, der durch gezielte Sabotage von IT-Systemen, durch Datenabflüsse oder gar durch die Manipulation von Vorgängen potentiell entstehen könnte, ist unermesslich – sowohl für die betroffenen Menschen als auch für das Vertrauen in den Staat.

Um diesen Wandel zu schaffen, werden wir mit Bund, Ländern und Kommunen gemeinsam neue Lösungen finden müssen und dabei auch bereit sein, alte Strukturen zu überdenken, soweit sie eine einheitliche Antwort auf diese Gefahren verhindern. Ich appelliere daher an alle Beteiligten, sich ernsthaft und konstruktiv in diese Gespräche einzubringen und unterstütze ausdrücklich die Forderungen der Bündnisgrünen Bundestagsfraktion nach einem Kritis-Dachgesetz.

Doch auch ohne auf die großen bundesweiten Lösungen zu warten, haben wir hier in Brandenburg noch einige Aufgaben vor uns.

Für viele Bereiche des alltäglichen Lebens wurden in den letzten Jahren auf Bundesebene einheitliche Kriterien und Schutzziele für den Betrieb Kritischer Infrastrukturen festgeschrieben.

Für den Sektor Staat und Verwaltung sind jedoch die Länder am Zug, festzulegen, was zur kritischen Infrastruktur gehört und nach entsprechenden Standards geschützt werden muss. Hier braucht es dringend verbindliche Festlegungen, um die Basis für eine belastbare Bestandsaufnahme und notwendige Maßnahmen zu haben. Mit diesem Antrag bekennen wir uns dazu, dass Brandenburg hier zügig vorangeht.

Ein entscheidender Punkt für die Informationssicherheit ist der Umgang mit Sicherheitslücken in der genutzten Software. Im Idealfall erfährt man von einer Lücke dadurch, dass der Hersteller der Software die Nutzer*innen informiert und gleichzeitig ein Update bereitstellt. Doch selbst dieser grundlegendste aller Sicherheitsprozesse kann nicht als gegeben angesehen werden, solange wir nicht sicherstellen, dass die Aufrechterhaltung einer sicheren Infrastruktur in der Verwaltung die notwendige Priorität bekommt.

Ich möchte an dieser Stelle nur darauf verweisen, dass in Potsdam die betreffende Schwachstelle in der Software Citrix zwei Monate lang öffentlich bekannt war, bevor der besagte Vorfall geschah. Zwei Monate, in denen diese Lücke bekanntermaßen aktiv für Angriffe auf Citrix-Systeme in aller Welt ausgenutzt wurde, und in denen der Hersteller dringend zu Gegenmaßnahmen riet. Das alleine zeigt, wie groß die anzugehenden Baustellen sind. Denn niemand hier im Raum sollte sich der Vorstellung hingeben, dass Potsdam ein außergewöhnlicher Einzelfall wäre oder dass andere Städte und Gemeinden in Brandenburg in der Regel besser aufgestellt sind als die Landeshauptstadt. **Wen es trifft, das ist zu einem großen Teil Glück oder eben Pech. Und das ist meiner Ansicht nach etwas womit wir uns nicht abfinden sollten, wenn es um die grundlegende Integrität unserer Verwaltung geht.**

Deshalb fordern wir im Antrag die Landesregierung auch dazu auf, zu prüfen, wie wir die Kommunen noch besser bei der Gewährleistung von Informationssicherheit unterstützen können. Ein naheliegendes Beispiel wären sogenannte CERT-Dienste, also die konkrete Unterstützung durch Expert*innen bei Vorfällen und gezielte Information im Vorfeld um diese zu vermeiden.

Meine Damen und Herren, jetzt habe ich schon einige Punkte aufgezählt, die wir angehen wollen. Aber klar ist auch: die wirklich entscheidenden Stellschrauben sind die Fragen, Welche Programme und Technik wir einsetzen und ob wir die notwendigen Kompetenzen in der Verwaltung haben!

Wenn wir als Land digital souverän sein wollen, dann dürfen wir uns nicht von einzelnen Herstellern komplett abhängig machen. Das betrifft natürlich große außereuropäische Konzerne, die teils Schwierigkeiten mit unseren Gesetzen haben. Aber es gilt auch für das einzelne Fachverfahren, das nach Einführung integraler Bestandteil von Prozessen in einer Behörde wird. Deswegen braucht es dringend verbindliche Standards für die Beschaffung von Technik. In aller Regel sollte dabei versucht werden, freie und Quelloffene Software zu nutzen, bei der sichergestellt ist, dass der Staat als Anwender jederzeit Herr der eigenen Technik bleiben kann.

Die schwierigste und zugleich wichtigste Frage ist, wie wir die notwendige Expertise in die Verwaltung holen und dort halten. Wie schaffen wir es, die Bedingungen bereitzustellen um eine sichere Infrastruktur auf höchstem Niveau betreiben zu können? Wir geben mit diesem Antrag der Landesregierung auf, ein regelmäßiges Lagebild zum Stand der IT-Sicherheit sowie der personellen und finanziellen Ressourcen in diesem Bereich zu erstellen. Denn diese entscheidendste aller Stellschrauben darf keinesfalls aus dem Blickfeld geraten. Alle guten Konzepte helfen uns nicht, wenn wir nicht die Expert*innen, die dies tatsächlich umsetzen, halten und zusätzliche gewinnen können. Deshalb braucht es einen noch stärkeren Fokus auf Ausbildung, Anreize durch gute Arbeitsbedingungen und konkurrenzfähige Bezahlung. Hier werden wir in den kommenden Jahren noch einige Diskussionen zu führen haben, wenn wir das Problem wirklich ernst nehmen wollen.

Meine Damen und Herren, die Chancen der Digitalisierung sind unermesslich um die Aufgaben des Staates effizienter und besser zu erfüllen. Lassen Sie uns gemeinsam dafür sorgen, dass Brandenburg digitaler wird, dass wir diese Chancen nutzen. Dafür gibt es sehr viele konkrete Vorhaben und noch mehr gute Ideen. **Aber lassen Sie uns dabei nicht vergessen, dass es zum Bauen von Leuchttürmen zwingend ein solides Fundament braucht. Denn sonst besteht die Gefahr, nach einer stürmischen Nacht in einer Ruine aufzuwachen.**

Die Koalition geht mit diesem Antrag einen weiteren Schritt, um dieses Solide Fundament sicherzustellen. Ich bitte um Zustimmung.

Vielen Dank.

---

[1]

https://www.golem.de/news/nach-ransomware-katastrophe-rebuilding-landkreis-anhalt-bitterfeld-2112-162045-2.html

https://www.volksstimme.de/sachsen-anhalt/hackerangriff-anhalt-bitterfeld-verwaltung-hat-weiter-probleme-nach-ransomware-attacke-3402256

[2] Quelle für die Aussage, dass nach einem Jahr immer noch nicht alle Dienste online waren:

https://www.tagesspiegel.de/potsdam/landeshauptstadt/potsdamer-rathaus-zieht-bilanz-7961647.html Quelle für die Kosten:

https://www.tagesspiegel.de/potsdam/landeshauptstadt/cyberangriff-verursachte-kosten-von-82000-euro-7931017.html