LANDTAG NORDRHEIN-WESTFALEN
18. Wahlperiode

Drucksache **18/2543**

17.01.2023

Antrag

**der Fraktion der CDU und
der Fraktion BÜNDNIS 90/DIE GRÜNEN**

Aktuellen und zukünftigen Herausforderungen der IT-Sicherheit strukturiert begegnen

I. Ausgangslage

Digitale Systeme spielen täglich und fast überall in unserem Alltag eine große Rolle: Insbesondere Bürotätigkeiten sind ohne den Einsatz von Computer, Tablets, digitaler Prozesse und Anwendungen undenkbar. In der öffentlichen Verwaltung und der kritischen Infrastruktur, wie beispielsweise bei der Energieversorgung und in Krankenhäusern, spielt die Digitalisierung eine immer wichtigere Rolle.

Durch eine Vielzahl von Ereignissen in den vergangenen Jahren wurde deutlich, dass digitale Systeme einen starken Schutz brauchen. Cyberangriffe auf öffentliche und kritische Infrastrukturen bergen das Risiko, dass das alltägliche Leben aus den Fugen gerät oder sogar Menschenleben gefährdet werden. Die Landesregierung hat unter Federführung der Koordinierungsstelle Cybersicherheit die bundesweit erste Cybersicherheitsstrategie entwickelt. Insbesondere die Informationssicherheit der öffentlichen Verwaltung inklusive der Kommunen soll noch stärker in den Blick genommen werden. Denn das Risiko durch Ransomware-Angriffe steigt. Diese gefährden die Abläufe in Krankenhäusern, Unternehmen, öffentlichen Verwaltungen oder Hochschulen, indem Daten durch Verschlüsselung unzugänglich gemacht und ihre Freigabe erpresst werden.

Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) nimmt die Bedrohungslage der digitalen öffentlichen und kritischen Infrastrukturen in Deutschland seit Jahren zu. Digitale Netze dieser Einrichtungen sind tagtäglich Cyberangriffen ganz unterschiedlicher Akteurinnen und Akteure ausgesetzt. Diese erfolgen von Kleinkriminellen bis hin zu professionellen Hackerteams, die im Auftrag anderer Staaten Spionage und Sabotage betreiben. Die insbesondere durch die Corona-Pandemie fortgeschrittene Digitalisierung hat die Angriffsfläche für digitale Attacken vergrößert.

Der russische Angriffskrieg auf die Ukraine hat verdeutlicht, dass kritische Infrastrukturen häufig eine Zielscheibe für Angriffe sind. So gingen beispielsweise den aktuellen Attacken mit Drohnen monatelang Cyberattacken voraus. Dabei zeigt sich das Problem, dass häufig ein erfolgreicher Cyberangriff auf die kritischen Infrastrukturen eines Landes ebenfalls gefährlich für die Infrastrukturen anderer Länder ist. Denn die Wahrscheinlichkeit, dass die gleichen Komponenten zum Beispiel auch in den Infrastrukturen in Deutschland eingesetzt werden, ist hoch.

Eine neue IT-Sicherheitsstrategie entwickeln

Datum des Originals: 17.01.2023/Ausgegeben: 17.01.2023

Je größer der Anwendungsbereich digitaler Systeme in unserem Alltag wird und je weiter die Bedrohungslage steigt, desto höher ist die Notwendigkeit einer neuen Vorgehensweise. Es braucht hierfür eine Weiterentwicklung von IT-Sicherheitsstrategien, bei denen langfristige Entwicklungen vorausschauend einbezogen werden.

Die Aufgabe dieser IT-Sicherheitsstrategie wäre es, grundlegende Leitlinien und Technologieanforderungen festzulegen, die konstant im Dialog zwischen Sicherheitsexpertinnen und -experten, Entwicklerinnen und Entwicklern sowie Nutzerinnen und Nutzern weiterentwickelt werden. Gerade im IT-Bereich hat sich in den vergangenen Jahren gezeigt, wie notwendig es ist, Maßnahmen und Technologien kontinuierlich anzupassen und weiterzuentwickeln. Neue Sicherheitslücken erreichen IT-Verantwortliche fast täglich und erfordern, zusammen mit der schnellen Weiterentwicklung von Angriffen, dass vorhandene Systeme ständig in kurzen Zyklen überprüft und weiterentwickelt werden.

Gleichzeitig sind neue technologische Entwicklungen oft mit einer großen Unsicherheit behaftet, so dass unklar ist, wie sich die Bedrohungslage entwickelt. Disruptive Entwicklungen, deren Marktreife in den kommenden Jahren als wahrscheinlich gilt, wie beispielsweise Quantencomputer, erfordern schon heute eine Anpassung. Anforderungen an IT-Sicherheit festzulegen ist darüber hinaus komplex, da eine Kombination aus einer soliden technischen Sicherheit und sensibilisierten Nutzerinnen und Nutzern erforderlich ist. Oft ist noch die Informationslage, auf deren Basis Abschätzungen getroffen werden, uneindeutig.

Die Bedrohungslage ist aktuell sehr hoch. Um mögliche Schäden zu minimieren, müssen alle Betroffenen wissen, wie Angriffe unterbrochen und Systeme wiederhergestellt werden können. Dazu gehört auch die Handlungsfähigkeit im Falle eines kompletten Ausfalls der IT einer Verwaltung sicherzustellen. Auch das neue Anfahren aller Dienste nach einem Angriff oder das Ausschalten und Austauschen einzelner Dienste im Betrieb erfordert Übung, damit Wiederherstellungszeiten kurz gehalten werden können.

IT-Sicherheit wird auch im Hochschulumfeld eine immer wichtiger. Die Hochschulen sind täglich hunderten von Angriffen ausgesetzt. Diese sind in der Regel nicht erfolgreich. Zur Absicherung von Havariefällen haben sich die Hochschulen auf ein kooperatives Dienstekonzept für die Datensicherung geeinigt, welches Anfang 2022 gestartet ist. Ziel des Konzeptes ist, mit „Datensicherung.NRW“ eine verlässliche Datensicherung, die an wenigen Hochschulen betrieben werden muss, für alle Hochschulen anzubieten. Hierfür hat das Land Nordrhein-Westfalen zunächst rund 11 Millionen Euro für die Lizenzen und für einen ersten Backup-Standort an der RWTH Aachen zur Verfügung gestellt. Weitere Backup-Standorte sollen folgen.

Technologische Rahmenbedingungen beachten

Durch die aktuelle Lage wird deutlich, dass Abhängigkeiten von nur einem Land oder einem Unternehmen ohne gute, kurzfristig einsetzbare Alternativen gefährlich sein können. Aus diesem Grund muss digitale Souveränität – nicht zu verwechseln mit Protektionismus oder Autarkie – im Zentrum von Beschaffungsprozessen stehen. Dabei ist es auch wichtig, Informationen über die Software so vorliegen zu haben, dass eine politische Einflussnahme oder das absichtliche Platzieren von Sicherheitslücken ausgeschlossen werden kann. Bill of Materials oder Open Source sind Möglichkeiten, wie Software auf Einflussnahmen oder Sicherheitslücken hin überprüft werden kann.

Sicherheitsmaßnahmen müssen für Nutzerinnen und Nutzer einfach anwendbar sein, ansonsten werden unsichere Wege genutzt, um Maßnahmen zu umgehen. Nutzerinnen und Nutzer benötigen solide IT-Grundkenntnisse. Würden alle öffentlichen Angebote, vor allem jene zum

Selbststudium, zentral gebündelt und den Kommunalverwaltungen zur Verfügung gestellt, würde das die Kommunen entlasten und die Aktualisierung des Schulungsmaterials erheblich erleichtern.

Langfristige Entwicklungen rechtzeitig in den Blick nehmen

Die IT-Sicherheitsbranche befindet sich gerade in einem Paradigmenwechsel hin zum Zero-Trust-Prinzip. Anstatt von sicheren Netzwerkbereichen auszugehen, die durch eine einmalige Identifizierung benutzt werden können, geht man dazu über, dass sich Nutzerinnen und Nutzer stets wieder identifizieren müssen, wenn sie auf besonders sensible Daten zugreifen wollen. Manchen Nutzerinnen und Nutzer von Online-Shops ist dieses Prinzip bereits bekannt. Dabei kann die Zugangsbestätigung je nach Schutzbedarf unterschiedlich ausgestaltet sein. So kann auch die Sicherheit des Endgeräts überprüft werden, beispielsweise darauf, ob alle Aktualisierungen vorgenommen wurden, damit Sicherheitslücken geschlossen sind. In den USA soll Zero-Trust bis 2024 in allen Bundesbehörden ausgerollt werden.

Schon heute wird von Cyberangriffen berichtet, deren Ziel es nicht ist, unverschlüsselte Daten zu stehlen und sofort zu missbrauchen. Vielmehr sollen verschlüsselte Daten erbeutet und diese entschlüsselt werden, sobald Quantencomputer eine Marktreife erreicht haben, mit welcher klassische kryptographische Verfahren geknackt werden können. Es ist davon auszugehen, dass mit der Marktreife von Quantencomputern klassische Verschlüsselungsverfahren obsolet werden.

Daten der öffentlichen Verwaltungen haben allerdings einen sehr hohen Schutzbedarf. Deshalb ist es wichtig, frühzeitig mit Planungen zu beginnen, wie von klassischer auf Post-Quanten-Kryptographie umgestellt werden kann. Mit der Standardisierung von Post-Quanten-Kryptoalgorithmen durch das National Institute of Standards and Technology der USA im Juli 2022 ist es nun möglich, mit den Planungen zu beginnen, um Daten sicher vor der Entschlüsselung durch Quantencomputer zu machen.

II. Beschlussfassung

Der Landtag stellt fest, dass

- IT-Sicherheit eine unabdingbare Voraussetzung für die Funktionsfähigkeit von Demokratie und Rechtsstaat im digitalen Zeitalter und notwendige Voraussetzung für eine erfolgreiche Digitalisierung ist. Sie erlaubt Bürgerinnen und Bürgern, Wirtschaft und Verwaltung, sicherer im Internet unterwegs zu sein und vertrauensvoll online Verwaltungs- und Geschäftsprozesse zu nutzen.

- digitale Souveränität für Verwaltungen bedeutet, Wahlmöglichkeiten zwischen verschiedenen Anbietern von Hard- und Software zu haben, idealerweise mit Angeboten aus Deutschland oder der Europäischen Union, um damit technologisch unabhängiger zu sein.

- IT-Sicherheit und digitale Souveränität zusammen die Grundlage einer selbstbestimmten digitalen Verwaltung sind, die von Bürgerinnen und Bürgern vertrauensvoll genutzt wird.

Der Landtag beauftragt die Landesregierung,

- zu prüfen, wie Maßnahmen zur IT-Sicherheit in Landes- und Kommunalverwaltungen so strukturiert werden können, dass ein kontinuierlicher Prozess entsteht, in dem Sicherheitsmaßnahmen entsprechend dem PDCA-Zyklus fortlaufend überprüft, umgesetzt und weiterentwickelt werden.

- zu prüfen, ob ein Backupsystem für Land und Kommunen nach Vorbild der Hochschulen einen Mehrwert bringen kann.

- für den Bereich der Landesverwaltung Pläne, Maßnahmen und regelmäßige Übungen zur Reaktion auf Schadenslagen zu entwickeln, die eine zügige Rückkehr zum Normalbetrieb nach einem erfolgreichen Angriff ermöglichen, und dabei Strukturen und Kommunikation in Zuständigkeit oder Auftrag des Landes so zu vereinfachen, dass Reaktionszeiten auf mögliche Angriffe und Softwarelücken von wenigen Stunden ermöglicht werden.

- unter Berücksichtigung der technischen Kompetenzen des Bundesamtes für Sicherheit in der Informationstechnik ein Konzept erarbeiten zu lassen, wie sich neue technologische Entwicklungen besser im Voraus auf ihre Anwendbarkeit mitgedacht und bei Verfügbarkeit zügig in die bestehende digitale Infrastruktur eingearbeitet werden können, beispielsweise das Zero-Trust-Prinzip und Post-Quanten-Kryptographie, und wie kritische Softwarekomponenten in der Landesverwaltung in Zukunft im Hinblick auf IT-Sicherheit, aber auch auf die Möglichkeiten politischer Einflussnahme, umfassend geprüft und zertifiziert werden können. Dabei sollen Doppelstrukturen möglichst vermieden werden.

- ein Konzept erarbeiten zu lassen, wie vorhandene Sicherheitsmaßnahmen so vereinfacht werden können, dass sie für Benutzerinnen und Benutzer einfach zu verwenden sind, und daraus regelmäßige Awareness-Maßnahmen für alle Mitarbeitenden der Landes- und Kommunalverwaltungen abzuleiten.

- den BSI-Grundschutz in allen Teilen der Landes- und kommunalen Verwaltungen umzusetzen und Mitarbeiterinnen und Mitarbeiter entsprechend fortzubilden.

- eine Sicherheitskonferenz mit allen relevanten Akteurinnen und Akteuren abzuhalten, um einen Weg zu einem Kommunal-CERT 2.0 festzuschreiben, welches proaktiv die Sicherheitslage für die Kommunen im Blick behält, sie bei der Umsetzung des BSI-Grundschutzes berät und bei erfolgreichen Angriffen auf die IT unterstützt.

- zu prüfen, ob ein Förderprogramm zur Stärkung der Informationssicherheit in den Kommunen aufgelegt werden kann.

Thorsten Schick	Wibke Brems
Matthias Kerkhoff	Verena Schäffer
Dr. Jan Heinisch	Mehrdad Mostofizadeh
Gregor Golland	Dr. Julia Höller
Björn Franken	Michael Röls
Dr. Christos Katzidis	Julia Eisentraut
und Fraktion	und Fraktion