BESCHLUSS

des Präsidiums der FDP, Berlin, 13. November 2023

Cybersicherheit stärken – Resilienz gegen Cyberangriffe erhöhen

Cyberkriminalität stellt eine elementare Bedrohung für Wirtschaft, Politik und Gesellschaft dar. Laut einer Studie im Auftrag des Digitalverbands Bitkom entsteht der deutschen Wirtschaft durch Datendiebstahl, digitale und analoge Industriespionage und Sabotage ein jährlicher Schaden von 206 Milliarden Euro. Jedes zweite Unternehmen gab an, sich durch Cyberangriffe existenziell bedroht zu fühlen. Auch Verwaltung und Kommunen sind täglich Ziel von Cyberangriffen. So beeinträchtigt derzeit beispielsweise ein großangelegter Hackerangriff auf mehr als 70 Kommunen in Nordrhein-Westfalen die Handlungsfähigkeit der Bürgerämter. Online-Dienste sind blockiert und Gewerbeummeldungen können nicht verarbeitet werden. Für Bürgerinnen und Bürger stellt der Daten- und Identitätsdiebstahl, insbesondere durch Phishing-E-Mails, eine tagtägliche Bedrohung dar. Auch Behörden, Parteien und andere öffentliche Einrichtungen werden zunehmend in großem Stil Zielscheibe von Cyberangriffen.

Deutschland muss angesichts der sich weiter verschärfenden Gefährdungslage durch Cyberangriffe, die insbesondere auch von China und Russland ausgehen, wirksame Maßnahmen ergreifen, um seine Resilienz zu erhöhen. Dazu fordern wir Freie Demokraten:

1. Wir brauchen dringend Fortschritte bei dem im Koalitionsvertrag vereinbarten strukturellen Umbau der IT-Sicherheitsarchitektur. Das BSI soll als zentrale Cybersicherheits-Stelle zusätzliche Kompetenzen im Bund-Länder-Verhältnis erhalten und zu einer selbstständigen Bundesoberbehörde heraufgestuft werden. Derzeit ist zwischen BSI, Ländern und Kommunen nur eine ausnahmsweise und punktuelle Zusammenarbeit möglich. Diese Möglichkeiten wollen wir im Sinne einer wirksamen Gefahrenabwehr, eines verbesserten Informationsaustauschs und einer schnellstmöglichen Schließung von Sicherheitslücken erweitern. Das BSI soll zukünftig seine Aufgabe als oberste Cybersicherheitsbehörde eindeutiger im Interesse der IT-Sicherheit wahrnehmen können. Bestehende Interessenkonflikte mit den klassischen Sicherheitsbehörden gilt es aufzulösen, indem mehr Unabhängigkeit von der Aufsicht und Weisung durch das Bundesministerium des Innern und für Heimat herbeigeführt wird.
2. Weiterhin ist es in Deutschland Praxis, dass zur Ausnutzung durch Sicherheitsbehörden, kritische Schwachstellen offen bleiben bzw. zurückgehalten werden. Diese nutzen Sicherheitsbehörden für technisch komplexe Überwachungsmaßnahmen. Unter dem Strich gefährden offene Schwachstellen aber die IT-Sicherheit aller. Denn es kann nie ausgeschlossen werden, dass die offenen Lücken nicht auch bei Cyberkriminellen oder anderen feindlich gesinnten Akteuren bekannt sind und von diesen genutzt werden.

Alle staatlichen Stellen sollen deshalb zukünftig verpflichtet sein, ihnen bekannte Sicherheitslücken beim BSI zu melden. Das BSI hat dafür Sorge zu tragen, dass Schwachstellen immer schnellstmöglich geschlossen werden (durch Meldung an Hersteller oder Betreiber). Der Staat wird zukünftig keine Sicherheitslücken ankaufen oder offenhalten.

3. Durch eine Verfassungsänderung soll der Bund bundeseinheitliche Regelungen und Lösungen für die effektive Abwehr schwerwiegender, weiträumiger Cybergefahren und für die Zusammenarbeit mit den Ländern bei der Gewährleistung der Sicherheit der Informationstechnik erlassen können.
4. Alle staatlichen Stellen sollen verpflichtend regelmäßige, umfassende externe Sicherheitsüberprüfungen ihrer Hard- und Software sowie der Netzwerke durchführen. Durch sogenannte Penetrationstests können Sicherheitslücken frühzeitig erkannt und geschlossen werden, sodass Cyberangriffe verhindert oder zumindest erschwert werden. Bekannte Sicherheitslücken müssen dem BSI gemeldet werden.
5. Unsere digitale Infrastruktur muss besser geschützt werden. Deshalb sollen Unternehmen wie Huawei, die Einflussmöglichkeiten autoritärer Regime unterliegen, beim Ausbau der digitalen Infrastruktur wie dem 5G-Netz nicht beteiligt werden. Auch Abhängigkeiten gegenüber einzelnen Unternehmen sind zu vermeiden. Für bereits eingesetzte Hardware, die den oben genannten Kriterien entspricht, fordern wir eine Fade-Out-Klausel. Insbesondere im Bereich der kritischen Infrastrukturen darf es keine gefährlichen Abhängigkeiten geben.
6. Die Europäische Kommission muss beim Cyber Resilience Act (CRA) die richtige Balance zwischen mehr Cybersicherheit auf der einen und geringer Regulierung bzw. Bürokratie auf der anderen Seite finden. Zu viele Vorschriften würden Unternehmen unnötig belasten. Wir sind grundsätzlich davon überzeugt, dass Cybersicherheit am besten durch gemeinsame europäische Forschung und Know-how gestärkt werden kann.
7. Wissenschaft und Wirtschaft müssen stärker in den Austausch gehen und enger kooperieren. Denn Cybersicherheit ist zunehmend ein wichtiger Markt für die deutsche Volkswirtschaft. Wir sind führend in der Forschung in diesem Bereich. Je mehr Unternehmen direkt von der Grundlagen- bis zur anwendungsbezogenen Forschung miteinbezogen werden, desto besser.
8. Unsere Sicherheit muss durch eine engere Kooperation von ziviler und militärischer Forschung gestärkt werden. Das gilt insbesondere im Hinblick auf Gefahren aus dem Cyberraum. Dafür müssen Zivilklauseln und Kooperationsverbote von Forschungseinrichtungen mit der Bundeswehr aufgehoben werden.
9. Wir fordern die Bundesländer auf, eine flächendeckende und gemeinsam abgestimmte Verortung von Medien- und Digitalkompetenzen in den Schulen zu implementieren. Schülerinnen und Schüler müssen bestmöglich auf Gefahren im Cyberraum vorbereitet werden. Dazu zählt auch der vernünftige Umgang mit digitalen Medien.