Stiftung Neue Verantwortung

Mündliche Stellungnahme

27. Sitzung des Ausschusses für Inneres, Sicherheit und Ordnung (Berlin) am 11. Dezember 2023

Besprechung gemäß § 21 Abs. 3 GO Abghs
Schutz vor Cyberangriffen: Stand und Entwicklungen

Dr. Sven Herpig
Leiter für Cybersicherheitspolitik und Resilienz
Stiftung Neue Verantwortung e. V.

Sehr geehrter Herr Ausschussvorsitzender,
sehr geehrte Abgeordnete,
sehr geehrte Sachverständige,
sehr geehrte Zuschauende,

IT-Sicherheit ist eine der Grundlagen für eine funktionierende Digitalisierung der Verwaltung, und damit verbunden auch das Vertrauen von Wirtschaft und Gesellschaft in den Staat. Gleichzeitig ist gemäß unserer Bundessicherheitsbehörden die Bedrohungslage im und aus dem Cyberraum so hoch wie nie zuvor. Die Lage in Berlin wird kaum anders sein, als die Lage in Gesamtdeutschland – aber mit Genauigkeit wissen wir das nicht.

Während jede und jeder hier von den Vorfällen um berlin.de, das KaDeWe und das Kammergericht weiss, fehlt es an einem umfassenden Lagebericht für das Land Berlin. Ein solcher Lagebericht zu Cybersicherheit – der Kriminalität, Spionage und andere böswillige Aktivitäten aus und im Cyberraum zusammenfasst und analysiert – wäre jedoch notwendig, um entsprechende Handlungsoptionen abzuleiten. Ohne zu wissen, was gerade wirklich passiert, kann man nicht zielführend reagieren und noch viel weniger strategisch planen. Für einen solchen Lagebericht braucht es jedoch weitere Voraussetzungen.

Ein Lagebericht ist nur dann gut, wenn die Datengrundlage solide ist. Und um eine bessere Datengrundlage zu bekommen, müssten Unternehmen verpflichtet werden, IT-Sicherheitsvorfälle zu melden. Ausnahmen für Kleinstunternehmen muss es genauso geben wie niedrig-schwellige Meldemöglichkeiten mit ausreichenden Fristen für Unternehmen, die keine kritischen Dienstleistungen erbringen. Meldungen können zum

Beispiel über die Digitalagentur erfolgen, damit nicht jedes Mal zwingend das Legalitätsprinzip zum Zuge kommen muss, was bei Meldungen an die Polizeien der Fall wäre. Wenn die Vergangenheit ein Anhaltspunkt ist, wird es nicht zu viel führen, hier auf Freiwilligkeit zu setzen.

Eine weitere Voraussetzung für einen sinnvollen Lagebericht ist eine zentrale staatliche Stelle, bei der Informationen zusammenlaufen und wo sie ausgewertet werden können. In Berlin würden sich hierfür vor allem das Landeskriminalamt mit seiner zentralen Anlaufstelle Cybercrime und das Cyber Defence Center der Landesverwaltung Berlin mit seinem Security Operations Center und dem Computer Emergency Response Team anbieten. Das Defence Center wäre dann eine gute Wahl, wenn man breiter als nur über Cyberkriminalität nachdenken möchte - was definitiv anzuraten wäre. Zweifelsohne müssten an dieser Stelle noch weitere Befugnisse geschaffen werden, vor allem wenn man zum Beispiel zukünftig ein Mobile Incident Response Team schaffen möchte. Die zentrale staatliche Stelle für Cybersicherheit in Berlin könnte auch über andere staatliche Stellen auf Bundes- und Länderebene hinaus mit Akteuren aus Wirtschaft, Wissenschaft und Zivilgesellschaft Sicherheitspartnerschaften bilden, um zum Beispiel gemeinsam Cybersicherheitsübungen durchzuführen.

Sowohl die Vorfallmeldepflicht für Unternehmen und weitere Organisationen, als auch die Benennung einer zentralen Stelle für Cybersicherheit in Berlin – mit gegebenenfalls weiteren Befugnissen – wird einen Rechtsakt erfordern. Dieser wird gegebenenfalls auch deswegen unumgänglich werden, weil sich der IT-Planungsrat dagegen entschieden hat Kommunen über die Umsetzung der europäischen Richtlinie über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau mit einer rechtlichen Basisabsicherung zu versehen. Ob die Berliner Bezirke nun darunter fallen oder nicht ist meines Erachtens noch nicht final geklärt. Die Bezirke sind aber neben der Wirtschaft diejenigen Akteure, die am meisten unter der aktuellen Bedrohungslage leiden. Gleichzeitig ist das Funktionieren der Bezirke im Rahmen der Digitalisierung der Verwaltung elementar. Da sie vernetzt sind, braucht es ein einheitliches IT-Sicherheitsniveau für alle Bezirke in Berlin. Kurzum: Berlin braucht zeitnah ein IT-Sicherheitsgesetz.

Der Entwurf eines IT-Sicherheitsgesetzes für Berlin, die Überführung des Lagebilds in konkrete Handlungen zur Verbesserung der IT-Sicherheit, die klare Benennung und der Ausbau einer zentralen staatlichen Stelle für Cybersicherheit in Berlin, sowie die Anbindung an andere Länder, und dem Bund mit einer möglichen Zentralstellenfunktion beim

Bundesamt für Sicherheit in der Informationstechnik obliegt der Senatsverwaltung für Inneres und Sport – dort vermutlich der Arbeitsgruppe Cybersicherheit.

Ich möchte mit einem Appell an die Fachkräfteausbildung schließen. Alle die genannten Maßnahmen können nur dann vom Reißbrett in die Realität transportiert werden, wenn Wirtschaft und Staat ausreichend qualifizierte Menschen haben, die operativ tätig werden. Während Maschinelles Lernen hierbei unterstützen kann, wird uns Künstliche Intelligenz nicht retten. Laut der Cybersecurity Workforce Study fehlen in Deutschland derzeit 100.000 Fachkräfte in diesem Bereich. Hinzu kommen Qualifikationslücken, zum Beispiel bei digitaler Forensik. Berlin sollte die Aus-, Um-, und Weiterbildung bei IT-Sicherheit zu einer Priorität machen. Die Grundlagen dafür hat Berlin als starker Wissenschafts- und Industriestandort für Informationstechnologien allemal.

Ein Dank geht an die Community für die Unterstützung bei der Recherche und Analyse zu diesem Themenkomplex.

Es gilt das gesprochene Wort.

Weiterführende Informationen

1. Michelle Busch, Julia Handle und Philip Schönfelder (2023): Vernetzung und Standardisierung stärken – für eine wirksame Prävention und Abwehr von Cybersicherheitsvorfällen; PD - Berater der öffentlichen Hand
2. Grüne Berlin (2020): LAG-Beschluss vom 30.07.2020: IT-Sicherheit in Berlin stärken
3. Sven Herpig und Frederic Dutke (2023): Deutschlands staatliche Cybersicherheitsarchitektur – 11. Auflage; Stiftung Neue Verantwortung
4. ISC2 (2023): Cyber Workforce Study 2023
5. Julia Schuetze (2023): Cybersicherheitskompass; Stiftung Neue Verantwortung – Berlin
6. Julia Schuetze (2023): Kommunale Informationssicherheit und Resilienz – Eine Analyse des deutschen Ansatzes zur Förderung; Stiftung Neue Verantwortung und Konrad-Adenauer-Stiftung
7. Julia Schuetze (2018): Warum dem Staat IT-Sicherheitsexpert:innen fehlen; Stiftung Neue Verantwortung