Deutscher Bundestag
Ausschuss für Inneres und Heimat

Ausschussdrucksache
20(4)418 H

Christine Skropke

secunet Security Networks AG

Kurfürstenstraße 58

45138 Essen

E-Mail: christine.skropke@secunet.com

Öffentliche Anhörung: Handlungsfähigkeit der Strafverfolgungsbehörden sichern – Entscheidung des BMI bezüglich der polizeilichen Analyse-Software Bundes-VeRA

Montag, 22. April 2024, 14:00h bis 16:00h
Paul-Löbe-Haus, Raum E 800, Konrad-Adenauer-Str. 1, 10557 Berlin

**Sachverständigenstellungnahme von Christine Skropke,
Leiterin Public Affairs bei der secunet Security Networks AG**

Aufklärung zu möglichen finanziellen Interessensverknüpfungen:

Die secunet Security Networks AG war weder im Bereich der Projekte Polizei 2020 noch an der öffentlichen Ausschreibung zur polizeilichen Analyse-Software Bundes-VeRA beteiligt. Aufgrund der neuen Ausgangslage wurde secunet Anfang 2023 eingeladen, seine Expertise im Bereich IT-Sicherheit in die Interessensgemeinschaft NASA (Nationale souveräne Analyseplattform) mit einzubringen. Bei einer möglichen Pilotierung würde secunet einen entsprechenden Anteil im Projekt realisieren.

Gesamtgesellschaftliche Perspektive

1. Die Sicherheit und der Schutz der Bevölkerung gehören zu den Kernaufgaben des Staates. Die dafür zuständigen Behörden sollten mit allen verfügbaren modernen Technologien zur Unterstützung ihrer Arbeit ausgestattet werden können.

Technologische Grundvoraussetzungen

2. Ein Analyse-System für die Arbeit moderner Sicherheitsbehörden muss technologisch offen konzipiert werden, damit auch neue (Zukunfts-) Technologien eingebunden werden können. So kann sichergestellt werden, dass die Bedarfsträger auch langfristig stets über die erforderlichen Fähigkeiten zur bestmöglichen Erfüllung ihres Auftrages verfügen.

3. Nationale hoheitliche Bereiche müssen sicherstellen, dass Daten und Informationen sowie die Kontrolle über den Zugriff auf die Anwendungen stets mit der höchst verfügbaren und vertrauenswürdigen Sicherheitstechnologie vor Sabotage, Spionage und Datenmissbrauch geschützt sind. Die Software allein einmalig auf Sicherheit zu überprüfen, stellt keine ausreichende Vertrauenswürdigkeitsüberprüfung dar. Ebenso unerlässlich ist die Einbettung der Software in sichere Cloud- und Netzwerkinfrastrukturen.

4. Mit Blick auf den bspw. erst kürzlich verabschiedeten AI Act der Europäischen Kommission sind alle aktuellen gesetzlichen regulatorischen Vorgaben in Hard- und Software entsprechend zu erfüllen.

Industriepolitische Perspektive

5. Sicherheitspartnerschaft und Partner der nationalen Sicherheitsbehörden

   Deutschland verfügt über eine weltweit hoch geachtete und anerkannte Forschung im Bereich der Sicherheitstechnologien ebenso wie im Bereich KI – sowohl in der Grundlagenforschung als auch bei der angewandten Forschung. Zahlreiche Inkubatoren, gefördert durch das Bundesministerium für Bildung und Forschung (BMBF), unterstützen jungen kreative Köpfe, aus der Forschung heraus Unternehmen zu gründen.

   Gleichzeitig legen seit Jahren die Bundesregierungen verschiedenster Koalitionen in ihren Strategiepapieren fest, dass die Sicherheits- und Verteidigungsindustrie mit ihren unterschiedlichsten Kompetenzen zu den Schlüsseltechnologien für Deutschland gehören und die Unternehmen dieser Branchen national geschützt und gefördert werden müssen.

   Für ein Unternehmen sind Gründungsförderungen und Kapitalgeber wichtig, aber das wichtigste für die Weiterentwicklung wichtiger technologischer Lösungen und Anwendungen sind Beauftragungen. Nur so kann ein Unternehmen seine Technologien in die praktischen Anwendungen bringen und diese gemeinsam mit den Bedarfsträgern weiterentwickeln. So werden diese Unternehmen gleichzeitig wirtschaftlich stabil und stellen nationale Fähigkeiten hinsichtlich Know-how oder entsprechender Fachkräfte sicher.

   Daraus entstehen dann wichtige nationale oder vielleicht sogar europäische Öko-Systeme, die auch wertvolle Beiträge leisten, wenn es um das Setzen neuer technologischer Standards geht. Technologiehoheit und -vielfalt verhindern die Abhängigkeit von Drittstaaten oder einzelnen Anbietern (Vendor-Lock-in). So kann Deutschland digital souverän werden und bleiben.

Auszug aus der Nationalen Sicherheitsstrategie von 2023

a. „Cybersicherheit ist untrennbar mit unserer digitalen Souveränität verbunden. Dieser Anspruch wird uns bei der gezielten Förderung von Technologien und bei der Weiterentwicklung von Sicherheitsstandards leiten. Die Bundesregierung wird hierfür auch die Zusammenarbeit mit der Industrie in den relevanten internationalen Gremien stärken."

   (Quelle: Wehrhaft. Resilient. Nachhaltig. Integrierte Sicherheit für Deutschland – Nationale Sicherheitsstrategie, 2023, S. 59)

b. „Die Bundesregierung wird überprüfen, bei welchen Schlüsseltechnologien nationale und europäische Fähigkeiten zum Schutz unserer technologischen und digitalen Souveränität nötig sind. Die Bundesregierung wird gezielt Anbieter kritischer Schlüsseltechnologien mit geeigneten Maßnahmen, z. B. durch staatliche Ankeraufträge, unterstützen, um eigene Fähigkeiten zu Forschung und Entwicklung in kritischen Technologien zu erhalten und weiterzuentwickeln."
   (Quelle: Nationale Sicherheitsstrategie, S. 58)

c. „Die Bundesregierung wird die Cybersicherheitsstrategie der Bundesregierung weiterentwickeln und dabei auch die Cybersicherheit der Bundesverwaltung umfassend stärken."
   (Quelle: Nationale Sicherheitsstrategie, S. 61)

Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie (BMWK) von 2020

Strategiepapier zu Schlüsseltechnologien „Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie", Bundesministerium für Wirtschaft und Klimaschutz (BMWK), 2020, schreibt die relevanten Technologien (u.a. Krypto) und deren Erhalt in Deutschland vor. Darin enthalten ist nicht nur entsprechende Forschungsförderung, sondern auch der Erhalt der Industrien.

> „Die Verfügbarkeit der identifizierten sicherheits- und verteidigungsindustriellen Schlüsseltechnologien ist aus wesentlichem nationalen Sicherheitsinteresse zu gewährleisten, abhängig von der Einordnung der Technologie gegebenenfalls auch im Rahmen von europäischen/transatlantischen Kooperationen und diesbezüglichen bi- und multilateralen Vereinbarungen."
>
> (Quelle: Strategiepapier der Bundesregierung zur Stärkung der Sicherheits- und Verteidigungsindustrie, 2020, S. 3 mit Grafik)

Ähnliche Aussagen siehe auch:

- Cybersicherheitsagenda des Bundesministeriums des Innern und für Heimat (BMI)
- Digitalstrategie der Bundesregierung
- Verteidigungspolitische Richtlinien 2023 des Bundesministeriums der Verteidigung (BMVg)

6. Leider müssen wir als deutsche IT- und Sicherheitsindustrie zunehmend feststellen, dass diese Partnerschaften oder Förderungen in Form von Aufträgen an nationale Anbieter häufig nicht in Betracht gezogen werden. Dabei lässt das Europäische Vergabeverfahren eine rein nationale Vergabe bei „Ausschreibungen für die nationale Sicherheit“ formal zu (siehe Vertrag über die Arbeitsweise der Europäischen Union, kurz: AEUV, Art. 346).

7. Es fehlt an generell an einer langfristigen Bedarfsplanung. Das Projekt für die Analyse-Software Bundes-VeRA wäre prädestiniert, die o.g. nationalen Strategien in eine operative Wirtschaftspolitik umzusetzen. Daher verwunderte es, dass bei der Europäischen Ausschreibung:
    a. kein deutsches oder zumindest europäisches Konsortium/Anbieter ausgewählt wurden,
    b. oder, sofern die Fähigkeiten zum Zeitpunkt der Ausschreibungserstellung noch nicht sichtbar / verfügbar waren, die deutsche oder auch europäische Industrie nicht frühzeitig in die Bedarfsermittlung und deren möglichen Realisierung eingebunden wurden.

8. Auch auf europäischer Ebene lösen solche deutschen Vergabepraktiken Verwunderung aus. Gespräche auf Verbandsebenen mit bspw. der Generaldirektion Migration und Inneres der Europäischen Kommission (DG Migration and Home Affairs) haben ergeben, dass die EU sehr wohl auch finanzielle Fördermittel bereitstellen würden für innovative polizeiliche Technologieentwicklungen für die EU und ihre Mitgliedsstaaten.

9. Deutschland würde sich mit der Förderung deutscher Technologien insbesondere für Sicherheitsorganisationen in keiner Weise „beschädigen“. Stattdessen würde es auf exakt gleiche Strategien setzen, die in Staaten wie den USA, Korea, China oder Frankreich regelmäßig Anwendung finden. Palantir wurde seinerzeit vom Pentagon (Ministry of Defense), CIA und NSA finanziell gefördert, und sowohl für die Geheimdienste als auch für das Militär eingesetzt.

Fazit:

Das Programm P20 als Zukunftsprogramm der deutschen Polizei ist der Reset-Button für die IT-Infrastruktur der deutschen Polizei des 21. Jahrhunderts. Im Sinne einer nachhaltigen nationalen Industriestrategie sollte insbesondere bei den kritischen Teilprojekten, wie z.B. den Analyse- und Auswertefähigkeiten, auf digital souveräne Lösungen nationaler Hersteller gesetzt werden. Die Vergabe an außereuropäische Anbieter von Einzellösungen mag kurzfristig attraktiv erscheinen, ignoriert jedoch mittel- und langfristige nicht absehbare finanzielle, technische und letztlich auch (geo-)politische Risiken.