Stellungnahme von Dr. Sven Herpig[1], Leiter für Internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung, für das Fachgespräch des Bundestagsausschusses Digitale Agenda am 28. Oktober 2020 zum Thema "Datensouveränität im Zusammenhang mit dem Projekt GAIA-X, Datenräume und Datenstrategie".

Deutscher Bundestag
Ausschuss Digitale Agenda

Ausschussdrucksache
19(23)088

Die vorliegende Stellungnahme ist auf die impliziten und expliziten (vgl. u. a. Frage 14[2]) IT- und Cybersicherheitsfragestellungen des vorliegenden interfraktionellen Fragenkatalogs beschränkt. Marktpolitische, wettbewerbspolitische, industriepolitische und geopolitische Aspekte werden weitgehend außen vor gelassen.

[1] Stiftung Neue Verantwortung (2020): Experten-Profil von Dr. Sven Herpig

[2] "Inwiefern soll GAIA-X in Bezug auf IT- und Cybersicherheit besser geschützt sein, als nicht europäische Lösungen? Was soll GAIA-X mit Bezug auf IT-Sicherheit leisten können, was bestehende Angebote nicht abdecken? Inwiefern spielen „vorgeschaltete“ IT-Sicherheitslösungen Made in Germany eine Rolle?"

IT- und Cybersicherheit als Bestandteil von "Digitaler Souveränität"?

Die deutsche Debatte über "daten-", "technologische" und "digitale Souveränität" wird seit vielen Jahren geführt. Dabei hat sie bis heute keine nachhaltige, allgemeingültige Definition von "[Begriff] Souveränität" hervorgebracht. Der Begriff ist somit oft eine Projektionsfläche unterschiedlicher Interessen, die jeweils gemäß aktuellem Anlass und eigener Agenda genutzt werden. Zuletzt wurde dieser Zustand in den Workshops des Bundesministeriums des Innern, für Bau und Heimat im September und Oktober 2020 deutlich. Trotz explizitem Verweis darauf, dass noch keine allgemein akzeptierte Definition erarbeitet worden sei, wurde im Rahmen der Weiterentwicklung der Cybersicherheitsstrategie über "digitale Souveränität" gesprochen. Die Bundesregierung sollte daher – in Zusammenarbeit mit Wissenschaft, Wirtschaft und Zivilgesellschaft – an einer breit akzeptierten Definition des Begriffes arbeiten, bevor er im politischen und rechtlichen Diskurs genutzt wird. Wichtig ist hier vor allem ein klarer Bezug zu Staaten (Deutschland), Staatengemeinschaften (Europa) und zwischenstaatlichen Beziehungen (z. B. zwischen Deutschland und den Vereinigten Staaten). Es bedarf eines klaren Koordinatensystems für die Bewertung von Abhängigkeit, Interdependenz und internationaler Arbeitsteilung.

Grundlagen für jede Debatte über "Datensouveränität", "Datenräume", "Datenstrategien" o. Ä. sind neben der Verfügbarkeit von entsprechenden Daten, der Schutz der Datensubjekte und ihrer Grundrechte, der Datenschutz und die Datensicherheit. IT- und Cybersicherheit sind hierfür elementar.

Der letztjährige Diskurs über die Speicherung der Bodycam-Aufnahmen der Bundespolizei auf Amazon-Servern war exemplarisch für die Wirrungen der politischen Debatte bei diesem Thema. Obwohl Amazon Web Services das C5-Testat nach Cloud Computing Compliance Criteria Catalogue des Bundesamtes für Sicherheit in der Informationstechnik[3] erlangen konnte, wurde die Bundespolizei für die dortige Speicherung ihrer verschlüsselten Daten kritisiert. Basis der Kritik war, dass es sich hierbei um einen US-Anbieter handelt. Interessanterweise wurde jedoch keine Kritik am Einsatz der Bodycams des ebenfalls aus den Vereinigten Staaten stammenden Anbieters Motorola Solutions laut, dessen Produkte in unterschiedlichen deutschen Sicherheitsorganisationen eingesetzt werden[4].[5]

[3] Bundesamt für Sicherheit in der Informationstechnik (2020): Kriterienkatalog Cloud Computing C5
[4] move (2017): Bund setzt weiter auf TETRA-Lösung
[5] Der Einsatz von IT-Produkten amerikanischer Anbieter bei deutschen Sicherheitsbehörden geht aber weit darüber hinaus und beinhaltet auch stark in die Kritik geratene Unternehmen wie Palantir, siehe zum Beispiel: Jannis Brühl (2018): Palantir in Deutschland - Wo die Polizei alles sieht

Es ergeben sich aus dieser Debatte folgende Fragestellungen, die auch im Rahmen von GAIA-X diskutiert werden sollten:

1. Ist ein IT-Produkt per se sicherer, nur weil der Hersteller aus Deutschland oder Europa kommt?
2. Gibt es bei nicht-deutscher oder nicht-europäischer Herkunft der Hersteller einen Unterschied bzgl. der IT- und Cybersicherheit des IT-Produkts?
3. Gibt es Möglichkeiten IT-Produkte nicht-deutscher oder nicht-europäischer Hersteller im Sinne von IT- und Cybersicherheit sicherer zu machen?

1. Deutsche oder europäische IT-Produkte sind nicht automatisch sicherer

Nur weil IT-Produkte in Deutschland oder Europa entwickelt oder betrieben werden, sind sie nicht automatisch sicherer. Während entsprechende Regulierungen (z. B. Datenschutz-Grundverordnung) hier ein Indikator sein können, kommt es vor allem auf die Implementierung der IT-Sicherheitsmaßnahmen an (z. B. Security by Design).

Ein weiterer wichtiger Aspekt ist die Analyse der konkreten Gefährdungslage. Das bezieht sich zum Beispiel auf die Art der Daten, die mit dem IT-Produkt verarbeitet und gespeichert werden sollen und vor welcher Art von Angreifer:innen diese Daten geschützt werden sollen.

Gefährdungsmodelle beinhalten:
a) Schutz vor dem Zugriff durch Kriminelle
b) Schutz vor dem Zugriff durch dritt-staatliche Akteure[6]
c) Schutz vor dem Zugriff oder der Abschaltung durch den Betreiber und staatliche Akteure in der entsprechenden Jurisdiktion[7]
d) Schutz vor dem Zugriff durch den eigenen Staat[8]

Hierbei ist leicht zu erkennen, dass aus Sicht eines deutschen Unternehmens ein unsicheres europäisches IT-Produkt bei allen Gefährdungsmodellen versagen könnte, während ein sicheres außer-europäisches IT-Produkt möglicherweise lediglich beim Gefährdungsmodell c) versagt.

Objektiv betrachtet hat die korrekte Implementierung von entsprechenden IT-Sicherheitsvorgaben, wie zum Beispiel der C5-Katalog des Bundesamtes für Sicherheit in

[6] Beispiel: Daten einer deutschen Firma liegen auf einem amerikanischen Server und sollen vor chinesischen Cyberoperationen geschützt werden.
[7] Beispiel: Daten einer deutschen Firma liegen auf einem amerikanischen Server und sollen vor dem Zugriff des Betreibers, sowie dem Zugriff von US-Behörden geschützt werden.
[8] Beispiel: Daten einer deutschen Firma liegen auf einem amerikanischen Server und sollen vor dem Zugriff deutscher Behörden geschützt werden.

der Informationstechnik für den Bereich Cloud Computing, höchste Relevanz für die IT-Sicherheit eines IT-Produkts. Im Fall von GAIA-X würde das nicht nur für das Anwendungsportal und das Cloud Betriebssystem[9] gelten, sondern jeweils für alle in der Federated Cloud zusammengeschlossenen Rechenzentren.

2. Bei nicht-deutschen und nicht-europäischen IT-Produkten sind Details zum Herkunftsland und des Anbieterzugriffs relevant

Betrachtet man Gefährdungsmodell "c) Schutz vor dem Zugriff oder der Abschaltung durch den Betreiber und staatliche Akteure in der entsprechenden Jurisdiktion" genauer, könnte man fälschlicherweise zu dem Schluss kommen, dass für ein europäisches Unternehmen die Gefährdungslage bei allen nicht-europäischen Herkunftsländern der genutzten Lösungen gleich ist. Hier müssen jedoch weitere Faktoren, wie zum Beispiel internationale Abkommen über Datenzugriff – z. B. der CLOUD Act[10] – und Rechtsstaatlichkeit (Unabhängigkeit der Gerichte, Transparenz der Prozesse u. v. m.) berücksichtigt werden. Diese Aspekte sollten auch auf Basis des Anbieterzugriffs beurteilt werden, sprich u. a.: welche (Meta-)Daten liegen vor – und in welcher Region – und wie sind sie vor dem Zugriff durch den Anbieter geschützt, z. B. mittels Verschlüsselung.

Während Verschlüsselung von übertragenen und gespeicherten Daten ("data in transit" und "data at rest") auf nicht-vertrauenswürdigen Systemen sicher funktionieren kann, ist die sichere Verarbeitung von verschlüsselten Daten ("data processing"), z. B. mittels homomorpher Verschlüsselung, nur bedingt möglich. Jedoch ist gerade in diesen Bereichen die Abhängigkeit von nicht-deutschen oder nicht-europäischen Dienstleistern besonders hoch – beispielsweise beim Training von Modellen für Maschinelles Lernen.[11]

3. Deutsche oder europäische IT-Sicherheit kann bei IT-Produkten aus anderen Herkunftsländern "vorgeschaltet" werden

Die deutsche IT-Sicherheitsindustrie hat in der Vergangenheit gezeigt, dass es möglich sein kann, Sicherheitsmodule für Lösungen zu entwickeln, denen aufgrund ihres Einsatzzwecks in Verbindung mit dem Herkunftsland des Anbieters unter Umständen nicht vertraut wird. Beispiele in anderen Einsatzbereichen sind die Planungen zur "IP-Kryptolösung" von Rohde

[9] vgl. z. B. secustack (2020): SecuStack
[10] vgl. z. B. Netzpolitik.org (2020): Cloud Act
[11] Sven Herpig (im Erscheinen): Understanding the Security Implications of the Machine-Learning Supply Chain

& Schwarz für Cisco Router[12] und die SecuSUITE von Secusmart (jetzt Blackberry)[13] für Smartphones im behördlichen Einsatz.

Alle Elemente von GAIA-X müssen mindestens den gleichen IT-Sicherheitsstandard aufweisen, wie die anderen Anbieter am Markt. Andernfalls sollte geprüft werden, ob mittels Nutzung "vorgeschalteter" IT-Sicherheitslösungen die Nutzung bestehender Anbieter nicht zielführender wäre.[14] Hierbei ist auch ein entsprechender Entwicklungs- oder Anpassungszeitraum der IT-Sicherheitslösungen zu berücksichtigen. Offene Standards, (Free/ Libre) Open Source und Interoperabilität der Lösungen sollten hierbei eine zentrale Rolle einnehmen, da sie für einen dezentralen Aufbau und eine stetige Weiterentwicklung elementar sind.

IT-Produkte deutscher oder europäischer Hersteller sind nicht per se sicherer als andere. Die IT- und Cybersicherheit von GAIA-X, welche eine wichtige Grundlage für die Datennutzung darstellt, wird an der objektiven Erfüllung der IT-Sicherheitsvorgaben aller ihrer Einzelteile gemessen werden müssen.

Während Anwendungen zum sicheren Datentransfer und zur sicheren Datenspeicherung zwar relevant sind, ist sichere – souveräne – Datenverarbeitung, vor allem in Bereichen wie dem Training von Modellen für Maschinelles Lernen, unerlässlich für den Erfolg von GAIA-X. Sollte das nicht realisierbar sein, so müsste umgehend geprüft werden, inwiefern die Entwicklung und Anpassung von IT-Sicherheitslösungen, die eine solche Datenverarbeitung unter hohem Sicherheitsniveau auf Systemen anderer Anbieter ermöglichen, gezielt gefördert werden kann.

Kontakt

Dr. Sven Herpig
sherpig@stiftung-nv.de
@z_edian (Twitter)
Leiter für Internationale Cybersicherheitspolitik
Stiftung Neue Verantwortung

[12] Rohde & Schwarz (2015): IP-Kryptolösung von Rohde & Schwarz SIT und Cisco für ungebremsten Netzverkehr
[13] BlackBerry (2020): SecuSUITE Secure Messaging and Phone Calls
[14] Die Rolle von existierenden Zertifizierungen von Produkten dieser Anbieter sollte mit in Betracht gezogen werden.