Forschungs- und Entwicklungsprojekt „Digitale Souveränität" Made in Germany

Handlungsbedarf – Ziele – Sicherheits- und wirtschaftspolitischer Nutzen

Seit einigen Monaten wird in Deutschland ein intensiver politischer und gesellschaftlicher Diskurs über die Chancen und Risiken der Digitalisierung geführt. Dabei geht es auch darum, wie in einer digitalen Welt deutsches Know-how aus Wirtschaft und Wissenschaft effizient vor Wirtschafts-und Industriespionage geschützt und wie ein angemessener Schutz der Verbraucher gewährleistet werden kann.

1. Bedeutung der IT-Wirtschaft und IT-Sicherheit in Deutschland wächst

Die IT-Branche stellt wesentliche Schlüsseltechnologien des 21. Jahrhunderts bereit, von denen Wachstum und Innovation, aber auch Sicherheit und Vertrauen in Deutschland maßgeblich abhängen. Vor diesem Hintergrund hat die Bundesregierung die Digitale Agenda 2014-2017 vorgelegt. In der Agenda skizziert die Bundesregierung die Grundzüge der Digitalpolitik, die sich an den strategischen Kernzielen *Wachstum und Beschäftigung*, *Zugang und Teilhabe* sowie *Vertrauen und Sicherheit* orientiert und die die Menschen in den Mittelpunkt stellt. Als eines von sieben Handlungsfeldern kommt dem Themenfeld *Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft* eine besondere Bedeutung zu, weil es sich hierbei um zentrale Querschnittsthemen der Digitalisierung handelt, die in allen Handlungsfeldern der Digitalen Agenda berücksichtigt werden müssen (*Digitale Agenda für Deutschland*, S. 31). Eine Experten-Befragung im Rahmen des *Monitoring-Report Digitale Wirtschaft 2014* belegt dabei die besondere Bedeutung des Handlungsfeldes *Sicherheit, Schutz und Vertrauen für Gesellschaft und Wirtschaft*: Es wird von den Experten als wichtigstes der sieben Handlungsfelder der Digitalen Agenda priorisiert (*Monitoring-Report Digitale Wirtschaft 2014, S. 79)*. Das Bundeskabinett hat am 11.3.2015 das neue Forschungsprogramm zur IT-Sicherheit "Sicher und selbstbestimmt in der digitalen Welt" beschlossen. Es soll ressortübergreifend die Aktivitäten zur IT-Sicherheitsforschung bündeln und die Entwicklung sicherer, innovativer IT-Lösungen für Bürgerinnen und Bürger, Wirtschaft und Staat fördern.

2. Defizite im Bereich IT-Sicherheit und IT-Sicherheitsforschung

Wirtschaft und Wissenschaft in Deutschland haben sich bislang in ihren Forschungs- und Entwicklungsaktivitäten im Bereich IT-Sicherheit zumeist nur auf einzelne Aspekte fokussiert. Viele Komponenten wurden und werden darüber hinaus in den USA entwickelt. Forschung, Entwicklung und Fertigung von Computern, Servern und Speichersystemen sind weitgehend aus Deutschland verschwunden. Dadurch ist erhebliches Know-how aus Deutschland abgeflossen. Fujitsu hat als einziger Anbieter aus strategischen Gründen an Forschung, Entwicklung und Fertigung von Computern, Servern und Speichersystemen in Deutschland festgehalten - trotz der höheren Lohnkosten. Die besonderen Defizite im Bereich IT-Sicherheitsforschung zeigen sich, wenn man mögliche Einfallstellen auf IT-Systeme über den gesamten Prozess (Ende-zu-Ende) betrachtet, also Endgeräte, Transportweg und Rechenzentrum im Blick hat. Bislang wurden in Deutschland keine Technologien entwickelt, die in der Lage sind, die möglichen Einfallstellen umfassend zu schließen. Hier einige Beispiele möglicher Einfallstellen:

Endgerät:	▪ *BIOS kann Einfallstellen enthalten* ▪ *Webcam und Mikrofon (intern/extern) können aktiviert und gesteuert werden* ▪ *Hauptspeicher speichert Daten unverschlüsselt*
Transportweg:	▪ *Schwachstellen in aktiven / passiven Netzwerkkomponenten (Internet/LAN/WAN)*
Rechenzentrum:	▪ *Durch nicht durchgängiges Monitoring werden Hackerangriffe erleichtert; Logs können verfälscht werden* ▪ *Ausgehende Daten können abgefangen, mitgelesen und manipuliert werden* ▪ *Administratoren können auf sensible Daten unbemerkt zugreifen*

3. Forschungs- und Entwicklungsprojekt „Digitale Souveränität"

Fujitsu betreibt an den deutschen Entwicklungsstandorten in Augsburg, München und Paderborn Forschungs- und Entwicklungsaktivitäten für einen umfassenden IT-Sicherheitsansatz, der in Deutschland und Europa einmalig ist. Dieser soll für besonders schutzbedürftige Daten und Vorgänge eine bislang nicht erreichte Sicherheit bieten – vom Endgerät über den Transportweg bis hin zum Rechenzentrum. Derzeit haben die Entwickler und Ingenieure von Fujitsu die möglichen Einfallstellen bei Endgeräten, dem Transportweg und im Rechenzentrum identifiziert. Zudem haben sie bereits neuartige technische und organisatorische Maßnahmen konzipiert, um diese schließen zu können. Durch diese Basisarbeit hat sich Fujitsu einen erheblichen Wettbewerbsvorsprung in Deutschland und Europa erarbeitet.

Das Vorhaben "Digitale Souveränität" setzt hierauf auf und verfolgt die Zielsetzungen:

- sichere Anwendungsumgebungen zu schaffen, die auf bestehenden und damit potenziell unsicheren Infrastrukturen aufsetzen
- ein Höchstmaß an Sicherheit zu gewährleisten, ohne Abstriche bei Bedienkomfort und Performance machen zu müssen
- wichtige Basiskomponenten für ein funktionierendes Sicherheits- und IT-Ökosystem in Deutschland zu schaffen, auf denen insbesondere Start-Ups, Mittelstand oder wissenschaftliche Einrichtungen aufsetzen können.

Im Rahmen des Gesamtvorhabens „Digitale Souveränität" betrachtet Fujitsu vielfältige Einzelmaßnahmen und fügt diese zu einem schlüssigen Gesamtkonzept zusammen. Dabei kann Fujitsu sein umfassendes Know-how „Made in Germany" zu allen wesentlichen Einfallstellen (zum Beispiel BIOS, Hardware, Treiber, Betriebssystem, Betrieb) zielgerichtet einbringen. In dem Forschungs- und Entwicklungsprojekt sollen neuartige technische und organisatorische Maßnahmen entwickelt bzw. weiter entwickelt werden. Hier einige Beispiele:

Endgerät:	▪ *Abstraktion von Hardware und Betriebssystem sowie Monitoring der Schnittstellen und des Speichers* ▪ *Kapselung der Einfallstellen*
Transportweg:	▪ *Vollhomomorphe Ende-zu-Ende-Verschlüsselung* ▪ *Gesteigerte Verschlüsselungsstärke („äußerer" und „innerer" Schlüssel)*
Rechenzentrum:	▪ *Neuartige Mehrfaktorenabsicherung gegen Administratoren- und Hackerangriffe* ▪ *Durchgehendes Monitoring und Auditierbarkeit* ▪ *Durchgängige, automatisierte Verschlüsselung* ▪ *Verbesserter Schutz gegen verteilte Angriffe von außen* ▪ *Absicherung gegen Seitenkanalangriffe*

Fujitsu profitiert mit Blick auf die zu erbringenden Forschungs- und Entwicklungsaktivitäten davon, als eines der wenigen Unternehmen in Deutschland alle Kompetenzen - also Hardware- und Softwarebereitstellung, Prozesse, Qualitätssicherung, Service, Support und Betrieb - vernetzt aus einer Hand anbieten zu können. Zudem verfügt Fujitsu über jahrzehntelange, praxisbewährte Erfahrungen in den relevanten Themen und unterliegt keinen einschränkenden internationalen Reglementierungen, wie z. B. dem Patriot Act. Die Entwicklung einer Gesamtlösung könnte in einem Forschungs- und Entwicklungsprojekt abgeschlossen und dabei in konkreten Proof of Concept-Vorhaben (PoC) verifiziert werden. Da die Entwicklungsaufwände aufgrund des umfassenden Ansatzes sehr hoch sind und das Vorhaben eine besondere sicherheits-, gesellschafts- und wirtschaftspolitische Bedeutung entfaltet, wäre es im Sinne der Digitalen Agenda, wenn der Staat ein solches Vorhaben aufgreift und fördert. In der Digitalen Agenda heißt es hierzu: „Wir forschen für die Sicherheit der Anwenderinnen und Anwender und setzen die Ergebnisse in der Praxis um. Das Forschungsprogramm *Selbstbestimmt und sicher in der digitalen Welt* wird sich mit der IT-Sicherheit neuer Technologien und dem Schutz von Daten in der Welt von morgen befassen und nutzerfreundliche Lösungen entwickeln." (Digitale Agenda für Deutschland, S. 31).Genau darauf zielt das Forschungs- und Entwicklungsprojekt „Digitale Souveränität".

4. Beispielhafte Themenfelder

Ohne die Gesamtkomplexität des Projektes an dieser Stelle vollständig abbilden zu können, werden im Folgenden beispielhaft einige Felder der Forschungs- und Entwicklungsarbeit dargestellt.

4.1. Sichere, ergonomische und benutzerfreundliche Authentifizierung

Biometrie-Lösungen zur Authentifizierung sind zukunftsträchtig, weil sie höchste Sicherheit bieten und zugleich anwenderfreundlich sind. Eine besondere Bedeutung messen wir dem biometrischen Authentifizierungsverfahren über das Venenmuster der Handfläche zu. Bei diesem Verfahren werden die durchbluteten Handvenen per Infrarot erkannt. Die Lösung ist technisch robuster und sicherer als andere biometrische Kontrollen. Sie ist 10 Mal sicherer als ein Scan der Iris im menschlichen Auge, 100 Mal sicherer als die Authentifizierung über einen Fingerabdruck und 1.000 Mal sicherer als die Gesichtserkennung. Hinzu kommt, dass sie einfach zu benutzen ist und berührungsfrei funktioniert. Wie Biometrielösungen zur Authentifizierung effizient und kostengünstig in eine schlüssige Gesamtarchitektur aufgenommen und dabei alle Datenschutzaspekte angemessen berücksichtigt werden können - ein Aspekt, der insbesondere für KMUs wichtig ist - ist Gegenstand des Forschungs- und Entwicklungsvorhabens.

4.2. Sichere Anwendungsumgebungen auf Basis bestehender Infrastrukturen

Angesichts der zahlreichen Bedrohungen und der Vielzahl möglicher Angriffspunkte können Informationen nur dann angemessen geschützt werden, wenn schutzbedürftige Programme und Inhalte vom Rest der IT-Infrastruktur vollständig und mit höchst möglicher Sicherheit abstrahiert werden. Diese „Kapselung" ermöglicht sichere Anwendungen und eine sichere Datenübertragung selbst in einer unsicheren IT-Umgebung. Bestehende Hardware und Netzwerk-Infrastrukturen können somit weiterhin genutzt werden. In dem Forschungs- und Entwicklungsprojekt soll aufgezeigt werden, wie eine solche Abstrahierung für spezielle Anwendungen realisiert werden kann, ohne dass Bedienkomfort und Performance leiden.

4.3. Ende-zu-Ende-Verschlüsselung von Daten mit erhöhter Verschlüsselungstiefe

Die sichere Übertragung zwischen Endgerät und Server ist ein weiterer Schlüsselfaktor, weil es hier eine Vielzahl möglicher Angriffspunkte gibt – speziell über mobile Anwendungen. Hier sind neue Sicherheitskonzepte gefragt, die über den heutigen Stand der Technik oder auch Konzepte wie das jüngst diskutierte nationale oder europäische Routing hinausgehen. Ein wichtiges Tätigkeitsfeld liegt deswegen in der Entwicklung neuer, umfassender Verschlüsselungsverfahren vom einen Ende der Verbindung bis zum anderen – und zwar als vollhomomorphe Ende-zu-Ende-Verschlüsselung. Die homomorphe Verschlüsselung bietet den Vorteil, dass die Daten auch für den Cloud-Dienstleister nie im Klartext vorliegen. Alle Berechnungen werden mit den verschlüsselten Daten durchgeführt. Dieses Verfahren erscheint derzeit im praktischen Einsatz limitiert, da die Daten nach einer gewissen Anzahl von Operationen verrauschen. Die vollhomomorphe Verschlüsselung wird deswegen von vielen Experten noch als Zukunftsmusik betrachtet. Fujitsu kann hier auf ein breites Know-how aufsetzen – ein Patent befindet sich in der Anmeldung.

5. Ökosystem für Deutschland schaffen – Standort Deutschland stärken

Auf Basis der zu entwickelnden Lösung ist es möglich, der deutschen Wirtschaft sowie Verbrauchern sichere IT-Umgebungen zur Verfügung zu stellen, ohne dass wesentliche Investitionen in neue IT-Infrastrukturen erforderlich werden. Damit lässt sich das Spannungsfeld der digitalen Konvergenz zwischen wirtschaftlichem Wachstum, Freiheit und Sicherheit bestmöglich auflösen. Für Unternehmen und Institutionen kann auf diese Weise eine „Plattform" zur Entwicklung und Integration ihrer Prozesse und Services geschaffen werden, die auf dem Austausch schützenswerter Daten und Informationen basieren (im Sinne von „Privacy by Design" und „Privacy by Default"). Zugleich könnten mit einem solchen Forschungs- und Entwicklungsprojekt wichtige Voraussetzungen für die weitere Entwicklung der deutschen IT-Wirtschaft und den zielgerichteten Ausbau des IT-Standortes Deutschlands im Sinne der Digitalen Agenda geschaffen werden. Ein wichtiges Ziel lautet dabei, Wettbewerbsvorteile für den Wirtschaftsstandort Deutschland zu schaffen, das Thema IT-Sicherheit als Standortvorteil für Deutschland auszubauen und in den europäischen Prozess einzubringen.

Digitale Souveränität "Made in Germany" ermöglichen:
Sicherheit aus der Sicht des Nutzers ganzheitlich betrachten, für eine einfache, hoch verfügbare Bereitstellung sorgen, die Nutzer zielgerichtet aufklären und eine anforderungsgerechte, abgestufte Sicherheit ermöglichen.

Chancen für Deutschland nutzen – Grundlagen für eine europäische IT-Strategie schaffen

Das Forschungs- und Entwicklungsprojekt „Digitale Souveränität" kann wesentliche Impulse liefern, innovative IT-Sicherheitslösungen in Deutschland zu entwickeln. Die IT-Sicherheitsanforderungen und -Bedürfnisse von Wirtschaft, Wissenschaft, Verwaltung und Verbrauchern werden aufgegriffen und können mit einem abgestuften Konzept bedient werden. Auf diese Weise kann ein entscheidender Beitrag zur Stärkung des IT-Wirtschaftsstandortes geleistet und Impulse zur Förderung der IT-Wirtschaft gegeben werden. Zugleich können die Voraussetzungen für Ansiedlungen und eine neue Gründerszene deutlich verbessert werden. Mit Blick auf die Cyber-Sicherheit in Deutschland und Europa können damit bestehende Defizite aufgeholt, die Wettbewerbsfähigkeit und Vertrauenswürdigkeit der IT-Industrie gestärkt, der Binnenmarkt für IT-Sicherheitsprodukte gefördert sowie weitere Forschung und Entwicklung im Bereich der IT-Sicherheit belebt werden.

Kontakt:
Fujitsu Technology Solutions GmbH
Jochen Michels
Mies-van-der-Rohe-Straße 8, 80807 München
Telefon: 0176 – 1042 4180
E-Mail: jochen.michels@ts.fujitsu.com
Website: www.fujitsu.com/de