ZVEI: Die Elektroindustrie

Diskussionspapier

Digitale Souveränität

Debatte über einen besonnenen Umgang mit internationalen Herausforderungen und die Stärkung des Industriestandorts Deutschland

Juni 2015

Zentralverband Elektrotechnik- und Elektronikindustrie

Impressum

Digitale Souveränität
Debatte über einen besonnenen Umgang mit internationalen Herausforderungen und die Stärkung des Industriestandorts Deutschland

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main
Telefon +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org

Verantwortlich:
Lukas Linke

Redaktion:
Arbeitskreis Cybersicherheit:

Sebastian Barchnicki	if(is) – Institut für Internet-Sicherheit Teletrust – Bundesverband IT-Sicherheit
Michael Barth	Genua
Jürgen Carstens	Rohde & Schwarz
Sebastian Glatz	ZVEI
Steffen Heyde	Secunet
Dr. Wolfgang Klasen	Siemens
Lukas Linke	ZVEI
Wolf-Rüdiger Moritz	Infineon
Dr. Holger Mühlbauer	Teletrust – Bundesverband IT-Sicherheit
Holger Pösken	Nexans
Günther Weber	Deep Innovation

Das Diskussionspapier entstand in enger Abstimmung mit dem Teletrust – Bundesverband IT-Sicherheit.

Juni 2015

Inhalt

Worum geht es?

Die zunehmende Digitalisierung und Vernetzung aller Lebensbereiche, insbesondere der Wirtschaft, Verwaltung und kritischen Infrastrukturen bietet Unternehmen gute Chancen, ihr Know-how in neue Technologien und Dienstleistungen umzusetzen. Andererseits erhöht dies die Abhängigkeit der Unternehmen untereinander sowie gegenüber Dienstanbietern. Gleichzeitig steigt das Risiko, durch unbeabsichtigte oder gezielte Fehlfunktionen und Manipulationen von sensiblen Daten, zum Beispiel bei einer Fehlsteuerung von Industrieanlagen, erhebliche Schäden zu erleiden.

Als Träger von Spitzen-Know-how steht die deutsche Industrie im Fokus der internationalen Wirtschaftsspionage und Cyberkriminalität. Nach Einschätzung des Präsidenten des Bundesamtes für Verfassungsschutz liegen die jährlichen Schäden für deutsche Unternehmen bei mindestens 50 Milliarden Euro. Die Sicherheit der Datenübertragung und -verarbeitung wird vor diesem Hintergrund zum strategischen Faktor für den Erhalt des Industriestandorts Deutschland.

Der heutige Datenverkehr basiert auf Internetdatenknotenpunkten wie „Decix“ in Frankfurt am Main oder „Linx“ in London, auf Routern, Switches und Prozessoren, Übertragungsmedien, eigenen oder externen Cloud-Diensten sowie Betriebssystemen, Browsern und komplexer Anwendungssoftware.

Alle diese Bereiche sind neuralgische Punkte für die Gewährleistung der Vertraulichkeit, Integrität, Authentizität und Verfügbarkeit von Daten. Sie befinden sich technologisch im Wesentlichen unter der Kontrolle von außereuropäischen Anbietern. Ihre Absicherung ist von strategischem Interesse für die deutsche und europäische Gesellschaft. Entsprechend ist mit besonderem Nachdruck zu diskutieren, welche Bedeutung die auf Anwendungsebene bestehende Abhängigkeit der deutsch-europäischen Gesellschaft von Technologien Dritter hat. Wie lässt sich in diesem Zusammenhang die Digitale Souveränität durchgängig und verlässlich gewährleisten?

Die notwendige Debatte muss dabei die Realität der bestehenden internationalen Herausforderungen einbeziehen. Dass unberechtigte Datenzugriffe über die internationalen Datenknotenpunkte erfolgen und es auf fast allen Anwendungsebenen Bestrebungen gibt, Schwachstellen zu implementieren oder auszunutzen, haben unter anderem die öffentlich gewordenen Programme „Prism“ und „Tempora“ deutlich gemacht. Es ist anzunehmen, dass die gewonnenen Informationen auch

zum Zwecke der Wirtschaftsspionage eingesetzt werden. Die Sicherheit der Datenkommunikation muss als permanente Herausforderung verstanden werden.

Grundsätzlich ist der Staat für die Bereitstellung und Absicherung von für die Gesellschaft wichtigen Funktionen und Infrastrukturen verantwortlich. Dies frei und selbstbestimmt zu gestalten, gilt im allgemeinen politischen Sinne als Souveränität. Im Zuge der zunehmenden Komplexität der Infrastrukturen bedarf es einer intensiven Zusammenarbeit von Politik und Industrie, um diese Souveränität zu gewährleisten. Das kann aber nicht die Abschottung von Internetinfrastrukturen oder globalen Märkten bedeuten.

Definition

Digitale Souveränität beschreibt die Fähigkeit, die Vertrauenswürdigkeit, Integrität, Verfügbarkeit der Datenübertragung, -speicherung und -verarbeitung durchgängig kontrollieren zu können. Entsprechend muss bewertet und sichergestellt werden, dass keine technischen Mittel im Kommunikationsnetzwerk vorhanden sind, die unberechtigten Zugriff, Veränderung oder Weiterleitung der Daten zulassen. Dies kann auf Produktebene grundsätzlich durch drei Optionen erreicht werden:

a) vertrauenswürdige Entwicklung und Produktion aller verwendeten Komponenten (Theorie)
b) Kombination vertrauenswürdiger Sicherheitskomponenten mit Drittkomponenten
c) verlässliche Evaluierung der verwendeten kritischen Komponenten

Digitale Souveränität bemisst sich durch den Grad der Selbstbestimmtheit und Kontrolle über die jeweiligen Glieder der Datenkette: Erhebung, Übertragung, Verarbeitung und Speicherung. Digitale Souveränität beinhaltet nicht zwangsläufig das Streben nach Autarkie. Vollständig kontrollierte Systeme gemäß Option a) wären ineffizient und wirtschaftlich nicht abbildbar. Grundlage der Digitalen Souveränität ist somit, die Akteure zu einer bewussten Entscheidung zu befähigen, damit sie die Risiken einschätzen und über das Schutzniveau ihrer Datenkommunikation bedarfsgerecht entscheiden können.

Als ersten Schritt fokussiert das Diskussionspapier zunächst die technische Ebene der Digitalen Souveränität. Selbstverständlich ist für eine umfassende Stärkung der Sicherheit die Rolle der Menschen, Prozesse sowie die Robustheit und Reaktionsfähigkeit von Systemen einzubeziehen. Hierfür ist ein durchgängiges, konsistentes und fortlaufendes Sicherheitsmanagement erforderlich.

Leitlinien für die Digitale Souveränität

Ziel des ZVEI ist ein ergebnisorientierter Dialog bezüglich der Umsetzung der Digitalen Souveränität unter Einbeziehung der Anwender und sonstiger Stakeholder. Als Grundlage ist eine Road-Map zu erstellen, die diejenigen Technologiefelder aufzeigt, die zur Erlangung der Digitalen Souveränität beherrscht werden müssen. Ihre Entwicklung ist angesichts der Relevanz für den Industriestandort Deutschland eine gemeinsame strategische Aufgabe der Industrie und Politik.

Um ein effizientes Vorgehen zu gewährleisten, bedarf es einer Anforderungsanalyse:

1. **Bedarf**: Welche Technologien werden für die Digitale Souveränität benötigt?
2. **Verfügbarkeit**: Welche dieser Technologien können hierfür am Industriestandort Deutschland konkurrenzfähig und vertrauenswürdig realisiert werden?
3. **Hürden**: Warum kommt vorhandenes Spitzen-Know-how national/international nicht zum Einsatz?

Für die Umsetzung schlägt der ZVEI folgende Leitprinzipien vor:

- Vorhandene Stärken ausbauen
- Abhängigkeiten analysieren und Kompensationsmaßnahmen aufzeigen
- Potenziale feststellen und heben
- Strategische Bündelung gegenwärtiger Initiativen zur Erreichung der Digitalen Souveränität

Der Analyseprozess verlangt eine vorbehaltlose, ehrliche Evaluation der bisherigen Ansätze. Zu viel Energie, Geld und Zeit sind bezogen auf marktreife Anwendungen ergebnisarm investiert worden. Das heißt, dass der oftmals gewählte Fokus auf Grundlagenforschung und Breitenförderung konstruktiv zu hinterfragen ist. Dem existieren aus der Vergangenheit sehr erfolgreiche Beispiele wie die Halbleiter-Initiativen „Jessi“ und „Medea“, die die Machbarkeit des Aufbaus eines strategischen Industriesektors aufzeigen.

Angesichts der Sicherheitslage besteht umgehender Handlungsbedarf.

Handlungsempfehlungen zur Digitalen Souveränität

Als maßgeblicher Anwender nimmt die Politik zwangsläufig Einfluss auf die Marktentwicklung von Sicherheitslösungen. Der sich daraus ergebenden Verantwortung sollte die Politik in Form einer strategischen Industriepolitik für Deutschland und

Europa gerecht werden. Die Industrie leistet weiterhin ihren Beitrag durch die Bereitstellung und Anwendung von integrationsfähigen Sicherheitslösungen „Made in Germany“.

Gemeinsame Aufgaben Politik und Industrie

- Führen eines „Schnittstellen-Dialogs“ mit den internationalen Herstellern von Infrastrukturhardware für die Bereitstellung von vertrauenswürdigen Applikationsschnittstellen für Security-Komponenten und die Entwicklung von vertrauenswürdigen Architektur-Modellen.
- EINE strategische Plattform etablieren: Die bisherige Vielzahl von Initiativen ist weder effektiv noch effizient. Es bedarf eines fokussierten Austausches über systemische Fehlentwicklungen sowie über Handlungsbedarfe.
- Evaluierung der bisherigen Security-Forschungspraxis zur Stärkung einer unmittelbaren und nachhaltigen Verwertung der Forschungsergebnisse. Wirksamer als die bisherige Praxis ist eine anwendungsorientierte Förderung von Security-Investitionen.
- Verbesserung der beruflichen Aus- und Weiterbildung in Bezug auf den sicheren Umgang mit digitalen Technologien und moderner Kommunikationsmittel.

Aufgaben der Politik

- „Fördern UND Kaufen“: Wahrnehmung der Vorbildfunktion des Staates bei Beschaffungsvorhaben. Setzen von hohen Security-Anforderungen bei Ausschreibungen als Ergänzung zum Kriterium „Preis“, die von allen Anbietern zu erfüllen sind.
- Bewusster Einsatz von Security-Referenzprojekten in Heimatmärkten. Aufgrund ihrer Signalwirkung für ausländische Investoren dienen sie als zentrales Element der Wirtschafts- und Exportförderung über die gegenwärtige Messeunterstützung hinaus.
- Innovationsfördernde und schnellere Zulassungs- und Zertifizierungsprozesse für IT-Sicherheitsprodukte zur Förderung der Digitalen Souveränität.

Aufgaben der Industrie

- Bereitschaft der Industrieunternehmen auf oberster Ebene:
  - Informationssicherheit zur Chefsache zu machen,
  - sich umfassend und fortlaufend über die Security-Ausgangslage zu informieren,

  - daraus abgeleitete Maßnahmen im Sinne der langfristigen Unternehmensentwicklung beharrlich umzusetzen,
  - aktiv an der Erstellung von bewertbaren Lagebildern mitzuwirken und diese für übergreifende Vergleiche anonym und datenschutzkonform auszutauschen.
- Investitionen der Industrieunternehmen in die eigene Security-Infrastruktur durch technische, organisatorische sowie Weiterbildungsmaßnahmen.
- Bereitstellung und Verbesserung der Interoperabilität sowie Integrationsfähigkeit von Sicherheitstechnologien „Made in Germany".
- Verantwortung in der internationalen Standardisierung wahrnehmen, um die Anwendung und Übertragung von Sicherheitstechnologien zu erleichtern.
- Demonstration von Best Practice Beispielen, um die wirtschaftliche Umsetzbarkeit der Digitalen Souveränität überzeugend darzustellen.
- Zusage an die Politik als Partner im Sinne der gemeinschaftlichen Aufgabe „Digitale Souveränität" zur Seite zu stehen.

Über den ZVEI

Der ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V. vertritt die gemeinsamen Interessen der Elektroindustrie und der zugehörigen Dienstleistungsunternehmen in Deutschland. Rund 1.600 Unternehmen haben sich für die Mitgliedschaft im ZVEI entschieden. Die Branche beschäftigt in Deutschland über 845.000 Arbeitnehmer und weitere 680.000 weltweit. Der ZVEI repräsentiert eine Branche mit 172 Milliarden Euro Umsatz im Jahr 2014. Etwa 40 Prozent davon entfallen auf neuartige Produkte und Systeme. Jede dritte Neuerung im Verarbeitenden Gewerbe insgesamt erfährt ihren originären Anstoß aus der Elektroindustrie.