Positionspapier

Stärkung vertrauenswürdiger IT-Infrastrukturen in Deutschland und Europa

Ein wichtiger Beitrag zur Digitalen Souveränität

November 2015

Zentralverband Elektrotechnik- und Elektronikindustrie

Autoren

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
Günther Weber	Deep Innovation

Impressum

Stärkung vertrauenswürdiger IT-Infrastrukturen in Deutschland und Europa
Ein wichtiger Beitrag zur Digitalen Souveränität

Herausgeber:
ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main

Verantwortlich:
Lukas Linke, ZVEI
Telefon: +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org

Redaktion:
Arbeitskreis Cybersicherheit
Das Diskussionspapier entstand in Zusammenarbeit mit dem TeleTrusT – Bundesverband IT-Sicherheit.

November 2015

Inhalt

1. Worum geht es?

1.1. Stärkung der eigenen Kontrollfähigkeiten

In einer global vernetzten Welt bestimmen Funktionsfähigkeit und Vertrauenswürdigkeit der genutzten IT-Infrastruktur ganz wesentlich den Fortbestand von Unternehmen, Verwaltung und kritischen Infrastrukturen. Funktionsfähigkeit und Vertrauenswürdigkeit beruhen wiederum auf durchgängigen Kontrollmöglichkeiten aller sicherheitsrelevanten Systemkomponenten und Prozesse. Diese durchgängige Qualitätssicherung ist in Europa derzeit nur bedingt gegeben. Wichtige Schlüsselkomponenten wie z. B. Betriebssysteme, Rechner- und Steuerungsanlagen, Router und Firewalls kommen marktbeherrschend aus außereuropäischer Fertigung. Die fehlenden Evaluierungsmöglichkeiten während der Herstellungsprozesse müssen durch nachträgliche Tests und Begutachtungen kompensiert werden.

Nur aus einem vertrauenswürdigen Produktionsumfeld entstehen sichere Produkte. Dies ersetzt aber nicht die notwendige Sorgfalt hinsichtlich der Produktqualität. Das übergreifende Bild fassen der ZVEI und der TeleTrusT mit einem dreigliedrigen Ansatz zusammen:

Quelle: ZVEI

1.2. Wir brauchen eine gemeinsame Strategie

Digitale Souveränität kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden. Derzeit existieren zu viele Einzelinitiativen, die kaum Wirkung zeigen. Es bedarf einer Umsetzungsstrategie, die Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik und Industrie vornimmt. Die Politik ist aufgerufen, den Startimpuls für die Umsetzungsstrategie zu setzen und sie langfristig zu unterstüt-

zen. Andere Staaten verfolgen bereits konsequent entsprechende Umsetzungspläne. Demzufolge muss Europa seine Konkurrenzfähigkeit gegenüber anderen Regionen neu erlangen und erhalten.

1.3. EINE Plattform für Digitale Souveränität

Die Vielzahl der existierenden Gesprächsplattformen zu diesem Thema erschwert die Arbeit für Politik und Unternehmen gleichermaßen. Eine strategische Bündelung in einer Public-Private-Partnership mit einem Beratungsgremium würde zur Effizienzsteigerung und Ergebniserzielung beitragen. Aufgaben dieser Plattform sollten unter anderem die Priorisierung der Umsetzungsmaßnahmen, die Ausgestaltung der „Schnittstellendialoge“ mit internationalen IKT-Infrastrukturherstellern sowie die Folgeabschätzungen globaler Normungs- und Technologieentwicklungen sein. Folgende Kriterien sollte die Plattform erfüllen:

- Ausbau einer bestehenden Plattform; Integration bestehender Kreise
- Einbezug aller relevanten staatlichen Institutionen mit einem klaren Mandat durch die Bundesregierung
- Einbindung der Wirtschaft (Anwender & Hersteller) und Wissenschaft
- Fokus auf die Arbeitsebene, CEO-Ebene bestätigt Inhalte

1.4. Sicherheit muss international funktionieren

Der deutsche Markt bleibt auf Dauer zu klein für hiesige Sicherheitsanbieter, um eine ausreichende Marktstärke und Rentabilität zu erzielen. Um ihren Fortbestand zu sichern, sind die Unternehmen auf den internationalen Markt angewiesen. Deutsche Sonderlösungen sind wirtschaftlich nicht abbildbar. Lösungen zur Stärkung der Digitalen Souveränität, insbesondere im behördlichen Bereich, sollten sich an internationalen Standards orientieren und leicht für weitere Märkte übertragbar sein. Parallel steht die Politik als traditionell großer Auftraggeber für Sicherheitslösungen im Fokus, wichtige Impulse für das Exportgeschäft deutscher Unternehmen zu setzen.

1.5. Zielsetzung und Selbstverständnis des Positionspapiers

Das Positionspapier richtet sich primär an Politik, Ministerien und Behörden. Denn die Stärkung der Vertrauenswürdigkeit sicherheitsrelevanter IT-Infrastrukturen für Bürger, Staat und Wirtschaft ist eine gesamtgesellschaftliche Aufgabe. Entsprechend liefert der ZVEI mit dem Positionspapier einen Beitrag für eine übergreifende Industrieposition aus Sicht der Elektroindustrie. Ziel ist es, diese gemeinsam mit der Politik auf EU-Ebene einzubringen. Das Papier drückt das Selbstverständnis der deutschen bzw. europäischen Elektroindustrie aus, die global agiert und weltweit einsetzbare Ansätze benötigt. Deutsche Insellösungen oder Autarkiebestrebungen lehnen die ZVEI-Unternehmen ab. Insbesondere die Elektroindustrie kennzeichnet, z. B. in der Medizintechnik, eine Exportquote von bis zu 81,9 Prozent. Im Kern beruht die Stärke der Branche auf der Integration in offene, globale Wertschöpfungsnetzwerke.

1.6. ZVEI-Forderungen

Folgende Schritte sind zur Zielerreichung notwendig:

Prozess	Inhalt
Unterstützung der Bundesregierung bei der Erstellung einer Umsetzungsstrategie Aufbau einer Plattform Integration bisheriger Kreise und Arbeitsergebnisse in die Plattform Überprüfung und Einbindung relevanter Akteure auf Arbeits- und Leitungsebene Festlegung priorisierter Maßnahmen	Festlegung der sicherheitsrelevanten Bereiche Sondierung der hierfür maßgeblichen Technologiefelder, zum Beispiel der ○ Applikations- u. Datensicherheit ○ Transport- u. Netzwerksicherheit ○ Identitäts- u. Rechteverwaltung ○ Gerätesicherheit und Systemarchitektur Sondierung der Hindernisse für deutsch-europäische Anbieter. Anschließend Förderung ausgewählter Bereiche durch PPP-Projekte Anpassung des öffentlichen Beschaffungswesens

2. Grundlagen

2.1. Umgehender Handlungsbedarf

Dass unberechtigte Datenzugriffe über die internationalen Datenknotenpunkte erfolgen und es auf fast allen Anwendungsebenen Bestrebungen gibt, Schwachstellen zu implementieren bzw. auszunutzen, haben unter anderem die öffentlich gewordenen Programme „Prism“ und „Tempora“ verdeutlicht. Es ist anzunehmen, dass die Akteure die gewonnenen Informationen auch zum Zwecke der Wirtschaftsspionage einsetzen. Parallel globalisiert sich der Austausch über Angriffswege. Nachrichtendienste, staatlich geförderte sowie private Cyberkriminelle bündeln ihre Ressourcen und erreichen dadurch ein immer höheres Fähigkeitsniveau. Es gilt: Jede technische und organisatorische Schutzmaßnahme lässt sich mit einem entsprechenden Aufwand umgehen.

Angesichts der Sicherheitslage besteht umgehender Handlungsbedarf

2.2. Verständnis und Definition

Digitale Souveränität beschreibt die Fähigkeit, Vertraulichkeit, Integrität und Verfügbarkeit der Datenübertragung, -speicherung und -verarbeitung durchgängig gewährleisten zu können. Nur durch diese Fähigkeiten kann schergestellt werden, dass sichere Produkte entstehen. Unternehmen und Behörden müssen bewerten und sicherstellen können, dass keine technischen Mittel im Kommunikationsnetzwerk vorhanden sind, die einen unberechtigten Zugriff, eine Veränderung oder eine Weiterleitung der Daten zulassen. Hierfür sind aus Sicht des ZVEI drei Kompetenzen relevant:

Herstellungskompetenz für Schlüsselkomponenten im Sinne einer vertrauenswürdigen Eigenentwicklung und -produktion von IT-Sicherheitslösungen, sofern sie ohne tief greifende Eingriffe des Staates erreicht werden kann.

Beurteilungskompetenz bezieht sich auf die Identifikation und Evaluierung kritischer Komponenten von Fremdanbietern gemäß dem Betroffenheitsprinzip und dient dem Ziel, Bewusstsein für Schwachstellen und „Backdoors“ zu schaffen. Hierzu gehören z. B. eine Risikoanalyse und Penetrationstests. Dies ist eine gemeinsame Aufgabe von privaten und staatlichen Stellen mit dem Anspruch, Markttauglichkeit und Neutralität zu gewährleisten. Eine derartige Vertrauensinfrastruktur ist über die angestrebte Plattform zu entwickeln.

Prozesskompetenz ist die Fähigkeit, Systeme technisch und organisatorisch sicher betreiben und unterhalten zu können. Sie kann vollständig hergestellt oder eingekauft und abgestuft werden. Das Schutzniveau eingesetzter externer Produkte und Systeme lässt sich durch die Kombination mit vertrauenswürdigen Sicherheitskomponenten heben.

Digitale Souveränität bemisst sich folglich am Grad der Kontrolle über die jeweiligen Glieder der Datenkette. Ausgangspunkt ist, dass die Akteure bewusst und bedarfsgerecht über das Schutzniveau ihrer Datenkommunikation entscheiden. Angesichts vieler laufender Prozesse bzw. bestehender Infrastrukturen steht für die Anwender insbesondere die Prozess- und Beurteilungskompetenz im Fokus.

2.3. Rolle und Beitrag der Elektroindustrie

Die Elektroindustrie ist mit rund 851.000 Mitarbeitern und einem 14-prozentigen Anteil am deutschen verarbeitenden Gewerbe (Stand 2014) die zweitgrößte Industriebranche Deutschlands. Die Unternehmen sind weltweit Technologieführer in den Bereichen Fabrikautomation, Energie- und Medizintechnik sowie Automobilzulieferung. Übergreifend bilden ihre Daten und Steuerungssysteme die Intelligenz in Industrieanlagen, Wohngebäuden, Fahrzeugen und kritischen Infrastrukturen. Mit dem Wissen um die Steuerung und Vernetzung industrieller Hardware und Prozesse sichert die Branche die Grundlage für die starke Stellung der deutschen Fertigungsindustrie in der Welt. Angesichts der Bedeutung und des Volumens der durch sie gemanagten Industriedaten sind der Ausbau sicherer IT-Infrastrukturen und die Stärkung der Digitalen Souveränität insgesamt von hohem gesamtwirtschaftlichem Interesse für den Standort Deutschland und Europa.

2.4. Sicherheit muss als Prozess verstanden werden

IT-Sicherheit kann nicht als Ansammlung einzelner „sicherer“ Komponenten verstanden werden. Erst im Zusammenwirken von Prävention, Detektion und Reaktion in einem Gesamtprozess entsteht eine Sicherheitsarchitektur. Jede Architektur ist ihrer Konstruktion nach auf eine „bekannte“ bzw. „vorstellbare“ Gefahrenlage ausgerichtet und muss auf der Basis aktueller Ereignisse und Erkenntnisse stets dynamisch weiterentwickelt werden.

Prävention: Das existierende Sicherheitsniveau wird durch die Robustheit gegen unbekannte Angriffe bestimmt: Aus der Erfahrung heraus werden Schutzmechanismen für (zukünftige) Produkte, Lösungen und Anwendungsarchitekturen in der Hoffnung definiert, durch die Auswahl der Sicherheitsmaßnahmen potenzielle Angriffe abwehren zu können. Dabei bestimmt eine Bedrohungs- und Risikoanalyse das Ausmaß und die Güte der eingesetzten Sicherheitsmaßnahmen. Aus einem solchen Prozess können natürlich keinerlei Garantien für die zukünftige Standhaftigkeit von Sicherheitslösugen abgeleitet werden. Maßstab ist stets die Erfahrung aus der Vergangenheit und die subjektive Einschätzung der zukünftigen Bedrohungslage, d. h. die Einschätzung der Fähigkeiten, Motivation und verfügbaren Ressourcen potenzieller Angreifer.

Detektion: Durch Beobachtung des Systems im Betrieb sollen Anomalien, die auf Sicherheitsverletzungen schließen lassen, erfasst und ausgewertet werden. Auch hier stützt man sich auf Erfahrungswerte aus der Vergangenheit. Die Qualität ist stark von der Lern- und Veränderungsfähigkeit der Bewertungskriterien bestimmt.

Reaktion: Die Reaktion auf erfolgreiche Attacken gegen eine Sicherheitsarchitektur hat verschiedene Facetten. Neben der aktuellen „Schadensbearbeitung“ ist die Überprüfung der Sicherheitsarchitektur auf erkennbare Schwachstellen mit all ihren Maßnahmen, Methoden und Prozessen erforderlich. In diesem Sinne bleibt die Sicherheit prinzipiell auch ein sogenanntes „afterthought“, da unabhängig von der Existenz proaktiver Maßnahmen eine stabile 100-prozentige Sicherheit nicht zu erreichen ist.

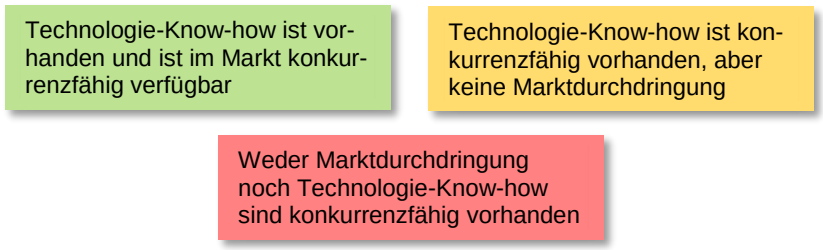
Digitale Souveränität kann nur erreicht werden, wenn alle Beteiligten diese drei Fähigkeiten kontinuierlich und umfänglich umsetzen.

3. Technologie und Fähigkeiten

Zur Stärkung der Digitalen Souveränität sind aus Sicht der Elektroindustrie und IT-Sicherheitswirtschaft folgende sechs Cluster relevant. Sie bilden die technische Basis für Datenerhebung, -transport und -verarbeitung.

Die Darstellung dient keiner detaillierten Bewertung. Sie fungiert als eine subjektive Einschätzung des Status Quo. Insofern sollen die Tabellen als unverbindliche Orientierung dienen. Eine systematische Erfassung des Status Quo sollte jedoch innerhalb der einzurichtenden Plattform erarbeitet werden.

Die Tabelle folgt einer Farbkodierung, die die Technologiekompetenz und Marktstärke aufzeigt:



Die daraus abzuleitenden Maßnahmen können de facto für jeden Teilbereich übergreifend zusammengefasst werden:

Grün: Kein direkter Handlungsbedarf für die Politik. Die Marktmechanismen reichen aus.

Gelb: Marktzersplitterung, fehlende Volumina auf dem Heimatmarkt, ungünstige Exportmöglichkeiten etc. erschweren die tatsächliche Etablierung von Spitzen-Know-how europäischer Unternehmen. Die Politik sollte durch Referenzprojekte, erleichterte Exportgenehmigungen und -unterstützung sowie ein bewusst in diesen Feldern eingesetztes Beschaffungswesen (Einsatz von hohen Sicherheitsanforderungen statt nur Kategorie Preis) unterstützend eingreifen. Die Industrie steht in der Verantwortung, Bedienungsfreundlichkeit, Service und Performance zu verbessern, um mehr Kaufanreize zu setzen.

Rot: In den Bereichen, in denen realistische Aufholchancen bestehen, sollte eine Intensivierung unternehmerischer und staatlich geförderter FuE-Anstrengungen erfolgen. In den Bereichen, in denen in sinnvoller Weise keine konkurrenzfähige Position aufzubauen ist, ist eine umfassende Bewertungskompetenz notwendig, um Sicherheitslücken identifizieren und beheben bzw. kompensieren zu können.

3.1. Applikationssicherheit

Applikationen bilden eine der wichtigsten Schnittstellen zum Nutzer und erfordern entsprechende Benutzbarkeit und Sicherheit, die zu den Nutzererwartungen passen müssen. Viele dieser Technologien spielen eine fundamentale Rolle für die Sicherheit des Nutzers, da sie z. B. zum Grundschutz von Systemen gehören.

Technologie	Zukunftsrelevanz	Bedrohungen	
App Sicherheit, Secure Marketplace	Wichtig aufgrund stetig steigender Anzahl mobiler Endgeräte	Einschleusen von bösartigen Apps, um Daten auf mobilen Geräten auszuspähen	
Exploit Protection sichere Applikation	Wichtig aufgrund starker Zunahme zielgerichteter Angriffe und der Verbreitung von 0-Day-Exploits gegen Unternehmen und Behörden	Angriffe durch infizierte Webseiten, Diebstahl lokaler persönlicher Daten	
Sicherer Browser, Remote Controlled Browser Systems (ReCoBS)	Hochsichere Ausführbarkeit von möglicherweise gefährlichen Daten in einem gesicherten Bereich ist auch in Zukunft wichtig	Einbruch in Systeme durch infizierte Webseiten	
Antivirus und Personal Firewall	Gehören zum sog. Grundschutz auf jedes PC-System und werden zukünftig zum Basisschutz gehören	Schadsoftware-Infektionen, ungewollte Verbindungen nach außen	

3.2. Datensicherheit

Datensicherheit umfasst die Sicherung von Informationen in allen Phasen der Verarbeitung. Dabei kann es sich um dauerhaft zu speichernde Daten oder aber auch die Übermittlung von Informationen an einen entfernten Ort oder befugte Personen handeln. Hierbei muss sichergestellt werden, dass Daten nicht ungewollt abfließen oder verändert, ausgewertet bzw. mitgelesen werden können.

Technologie	Zukunftsrelevanz	Bedrohungen	
Secure Instant Messaging (IM)	Durch Einzug von Web 2.0 in die Unternehmenskommunikation ist IM ein wichtiges Werkzeug	Mitschneiden und Auswerten aller Inhalte textueller Kommunikation	
Cloud Encryption	Immer mehr Organisationen machen von Cloud-Services Gebrauch. Insbesondere Industrie 4.0 setzt verstärkt auf Cloud-Dienste	Ausspähen von Daten und Diebstahl geistigen Eigentums durch Dritte (Firmen, Mitarbeiter, Geheimdienste)	
Virtuelle Schleuse	Da es immer häufiger zu Angriffen mit Schadcode kommt, sind Quarantänebereiche innerhalb von Netzwerken notwendig	Einschleusen von Schadcodes in beliebige Umgebungen mithilfe von Dokumenten oder Dateien	

E-Mail-Verschlüsselung	Die E-Mail gehört heute zur meistgenutzten Kommunikationsform in Unternehmen und die Nutzung steigt nach wie vor in allen Bereichen	Abfangen, Mitlesen und Manipulieren von E-Mail-Korrespondenz	
Data Leakage Prevention	Wissen wird heute durch Daten repräsentiert. Nur wenige Megabyte Datenverlust nach außen können verheerende Folgen für Unternehmen und Organisation haben	Abfluss hochsensibler Daten nach außen	
Verschlüsselung der Datenträger	Notebooks, Smartphones und PC-Systeme sind Geheimnisträger und beherbergen viele kritische schützenswerte persönliche Daten	Einsehen von Daten auf verlorenen oder gestohlenen Geräten durch Unbefugte	
Hardware-Sicherheitsmodul (HSM)	HSMs ermöglichen es, Daten innerhalb der Cloud zu verschlüsseln und trotzdem für die Weiterverarbeitung nutzbar zu machen. Dabei hat der Cloud-Dienst keinerlei Einsicht in die gespeicherten Daten und Vorgänge	Angriff auf vermeintlich sichere kryptografische Programmmodule	

3.3. Transportsicherheit

Der Bereich Transportsicherheit beschreibt die Sicherung der Kommunikation zwischen zwei Endpunkten mithilfe von kryptografischen Verfahren. Hiermit kann sowohl die sichere Informationsübertragung als auch die Legitimation der jeweiligen Kommunikationspartner durchgeführt werden.

Technologie	Zukunftsrelevanz	Bedrohungen	
chere Anbindung mobiler User	Die „Telearbeit“ erfreut sich steigender Beliebtheit. Arbeiten in Café und Zug oder an anderen öffentlichen Plätzen. Das Büro der Zukunft ist flexibel und schon heute häufig an keinen festen Ort gebunden	Abfangen sensibler Informationen und Abhören von Kommunikation	
Layer3-VPN	Verschiedene Standorte verschmelzen dank des Internets heute stark miteinander. Immer häufiger werden Orte an verschiedenen Punkten der Welt miteinander verbunden	Mitschneiden und Abfluss von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware	
Layer2-Encryption	Die immer höheren Bandbreiten und steigenden Teilnehmerzahlen erfordern nicht nur die Absicherung der Verbindungen verschiedener Endpunkte, sondern verlangen auch nach hohen Geschwindigkeiten	Mitschneiden und Abfluss von Daten durch Hintertüren und Sicherheitslücken in Netzwerkhardware	
Datendiode	In hochsicheren Bereichen werden auch zukünftig Produkte benötigt, die Netze effektiv so abschotten müssen, dass es keinerlei Möglichkeit für einen Rückkanal geben darf, sprich: Es dürfen nur Daten empfangen, aber niemals gesendet werden	Angriff auf Übermittlung und Empfang von Daten, die in eine Richtung an einen festen Empfänger transportiert werden	

3.4. Netzwerksicherheit

Bei der Netzwerksicherheit handelt es sich um Aspekte der sicheren Vernetzung und Maßnahmen für den geregelten Zugriff auf ganze Netze oder Teilbereiche von Netzwerken. Eingesetzt werden hierfür passive Systeme zur reinen Detektion und aktive Systeme, die über Abwehrmechanismen verfügen. Das Ziel ist, sensible und möglicherweise existenziell wichtige Organisationsdaten zu schützen und einen Einbruch in sensible Bereiche zu verhindern.

Technologie	Zukunftsrelevanz	Bedrohungen	
IPS/IDS	Künftig werden passive und aktive Systeme zur Detektion und Abwehr von Angriffen eine immer größere Rolle spielen. Sie sollten auf der einen Seite datenschutzkonform sein, auf der anderen Seite auch spezielle Angriffe (APTs) aufdecken	Angriffe von außen, die unmittelbar auf die Infrastruktur einer Organisation durchgeführt werden	
Remote Access / Secure VPN	Durch die zukünftige Dezentralisierung der Industrie in vielen Bereichen wird es notwendig sein, gesicherte temporäre Verbindungen z. B. für Wartungen zu nutzen	Belauschen und Manipulieren der Kommunikation zwischen Host und entfernter Maschine/Anlage	
Sichere Anbindung zwischen Anbieter und Anwender	Für eine sichere Verbindung zwischen Anbieter und Anwender werden auch in Zukunft Mechanismen erforderlich sein, die den Einsatz der sicheren Anbindung ermöglichen	Mitlesen und Auswerten von vertraulichen Daten	
Firewall	Immer mehr kritische Systeme werden an das Internet angekoppelt. Hierbei müssen effektive Maßnahmen zur Abwehr von Angriffen getroffen werden. Die eingesetzten Systeme müssen vertrauenswürdig sein	Angriffe von außen, Portscans, ungewollte Kommunikation von Diensten und Anwendungen nach außen	

3.5. Identitäts- und Berechtigungsverwaltung

Der Bereich der Identitäts- und Berechtigungsverwaltung berücksichtigt Möglichkeiten wie beispielsweise die Nutzung digitaler kryptografisch gesicherter Identitäten. Damit ist es möglich, sich beidseitig sicher gegenüber Dritten auszuweisen. Eine weitere Anwendungsmöglichkeit ist das Einleiten notwendiger Schutzmaßnahmen bei einem Verlust einer digitalen Identität oder eines mobilen Endgeräts, das an ein Netzwerk einer Organisation angekoppelt sein kann. Im Verlustfall kann dann sichergestellt werden, dass die sich darauf befindlichen Informationen nicht in falsche Hände geraten.

Technologie	Zukunftsrelevanz	Bedrohungen	
Device- und Portkontrolle	Mobile Datenträger werden immer kleiner und dabei immer leistungsfähiger, sprich sie bieten immer mehr Speicherplatz	Kopie vertraulicher Dokumente auf beliebige externe Datenträger	
Mobile Device Management (MDM)	In Organisationen werden immer häufig mobile Endgeräte eingesetzt. Geräte gehen verloren oder müssen bestimmten Vorgaben gerecht werden hinsichtlich Einstellungen und Sicherheit, die mithilfe von MDM-Systemen durchgesetzt werden können	Angriffe auf mobile Geräte aufgrund von Schwachstellen durch mangelnde Wartung oder Diebstahl	
Sicheres Logon (Smartcard etc.)	Feststellung von Identitäten einzelner Personen ist ein wichtiger Faktor in der Unternehmenssicherheit. Hierbei spielen Befugnisse für Maschinen oder Räumlichkeiten eine Rolle	Nicht autorisierte Nutzung von Geräten	
Authentifikation	Bei der Nutzung wichtiger Dienste im Internet muss sichergestellt werden, dass sich der genutzte Anbieter fälschungssicher gegenüber seinen Nutzern legitimieren kann, wie z. B. bei Onlinebanking oder E-Mail	Identitätsdiebstahl, Missbrauch fremder Identitäten	
Public-Key-Infrastruktur (PKI)	Die Industrie ist gerade dabei, einen möglichst hohen Grad an Digitalisierung zu erreichen. Schutz von Dokumenten, digitale Signaturen und Verschlüsselung von Dokumenten und Nachrichten sind bereits heute wichtige Faktoren in der Organisationslandschaft und gewinnen eine immer größere Bedeutung	Fälschen von Identitäten, um sich als Bank oder Institution auszugeben und das Vertrauen von Anwendern zu erschleichen, Mitlesen von Kommunikation, Brechen von Verschlüsselung	

3.6. Gerätesicherheit/Systemarchitektur

Der Bereich Gerätesicherheit und Systemarchitektur berücksichtigt die Zuverlässigkeit und Verlässlichkeit von Sicherheitssystemen und ihrer Architektur. Hierbei ist insbesondere der Anspruch im Hinblick auf die Vertrauenswürdigkeit besonders wichtig. Im Kern geht es dabei um die Durchsetzung von organisa-

torischen Unternehmensvorgaben, die Nutzung von Vertrauensankern, die Sicherung von Vertrauensketten und den Einsatz von Sicherheitskernen innerhalb komplexer Produkte.

Technologie	Zukunftsrelevanz	Bedrohungen	
Sichere Cloud-Plattform	Vertrauenswürdigkeit und Sicherheit mit einer hohen Resistenz gegen Angriffe, insbesondere bei mobilen Endgeräten, werden eine große Rolle spielen	Angriffe auf qualitativ mangelhafte Softwarekomponenten eines Systems	
Basistechnologie (Secure Execution Environment)	Als grundsätzliche Basistechnologie und Fundament komplexer Systeme für vertrauenswürdige Umgebungen z. B. im Bereich mobiler Endgeräte	Angriff auf Systemebene und Ausspähen von Daten durch Unbefugte	
Voll-Virtualisierung/ Trusted Computing, Separation	Die Konsolidierung zukünftiger Systeme dank immer leistungsstärkerer Hardware erfordert zunehmende Virtualisierung. Auch bei fehlenden Sicherheitsupdates durch Hersteller bei wichtigen Anlagen und Systemen ist Separation ein wichtiges Instrument für die Gewährleistung von Sicherheit	Infektion oder Angriffe auf einen Rechner kompromittieren das gesamte System	

4. Ansatzpunkt: IT Security Replaceability

Anwender in Deutschland und Europa sind weiterhin mit der Herausforderung konfrontiert, dass sie sich kein umfassendes Bild über die technischen (Security-)Auswirkungen der angebotenen IT-Produkte machen können. Hersteller aus dem Ausland sind selten bereit, ihre IT-Sicherheitsprodukte überprüfbar zu machen. Aus wirtschaftlichen Gründen ist es nicht sinnvoll, etablierte, aber nicht vertrauenswürdige Technologien und IT-Produkte (z. B. Router) vollständig durch eigene vertrauenswürdige Sicherheitsprodukte zu ersetzen. Dennoch kann die Digitale Souveränität gestärkt werden. Ein erster Ansatzpunkt ist die „IT Security Replaceability“.

Die „IT Security Replaceability“ beschreibt die Möglichkeit, Schlüsselkomponenten und Sicherheitsanker bestehender Produkte gegen vertrauenswürdige Bestandteile anderer Anbieter auszutauschen. Über die Bereitstellung entsprechender Schnittstellen und Austauschmöglichkeiten ist mit den Anbietern ein Dialog zu führen. Im Rahmen dieses „Schnittstellen-Dialogs“ sollte die Zielsetzung ebenso klar definiert werden wie auch das Vorgehen im Falle eines Scheiterns der Gespräche. Wichtig ist dabei die Steuerung dieses Prozesses durch die geforderte Umsetzungsplattform. Sie sollte als klarer Ansprechpartner und als treibende Kraft von Politik und Industrie fungieren.

5. Empfehlungen zur Umsetzung der Digitalen Souveränität

Als maßgeblicher Anwender nimmt die Politik zwangsläufig Einfluss auf die Marktentwicklung von Sicherheitslösungen. Zusätzlich besitzt sie eine Vorbildfunktion. Der sich daraus ergebenden Verantwortung sollte sich die Politik in der Form stellen, dass sie ein Beschaffungswesen betreibt, das neben der Beachtung von Kostenaspekten hohe Sicherheitsstandards für alle festschreibt. Die Industrie leistet hingegen ihren Beitrag durch die Bereitstellung und Anwendung von integrationsfähigen Sicherheitslösungen „Made in Germany“.

5.1. Gemeinsame Aufgaben

Führen eines „Schnittstellen-Dialogs“ zum Thema „IT Security Replaceability“ mit den internationalen Herstellern von IKT-Infrastrukturkomponenten (Hardware und Software), die in sensiblen Umgebungen eingesetzt werden. Ziel ist die Bereitstellung von vertrauenswürdigen Applikationsschnittstellen für Sicherheitskomponenten und die Entwicklung von vertrauenswürdigen Architekturmodellen. Der Dialog ist übergreifend für Europa zu führen. Angesichts der Relevanz des Anliegens für den europäischen Markt ist eine hohe politische Unterstützung maßgeblich.

Etablierung EINER strategischen Plattform: Die bisherige Vielzahl von Initiativen ist weder effektiv noch effizient. Es bedarf eines fokussierten Austauschs über systemische Fehlentwicklungen sowie über Handlungsbedarfe. Folgende Punkte sollten als Orientierung für die Ausrichtung dienen:

- Gemeinsame Besetzung aus Politik und Industrie (Hersteller + Anwender)
- Behörden- und ressortübergreifende Zusammensetzung (BMWi + BMI) mit einem klaren Mandat der Bundesregierung insgesamt
- Verortung bei einem Ministerium, das die Gesamtkoordinierung übernimmt und andere Stellen gleichberechtig einbindet
- Die Plattform sollte als zentraler Ansprechpartner für das Thema nach innen und außen dienen, vergleichbar mit der Plattform Industrie 4.0
- Fokus auf Arbeitsebene, Ergebnisse werden auf CEO-Ebene bestätigt
- Aufgaben:
    - Monitoring und Konsequenzenanalyse von internationalen Technologie- und Normungsentwicklungen,
    - Entwurf einer Umsetzungsstrategie (Zielsetzung + Umsetzungsschritte) und Kontrolle der Umsetzung.

Evaluierung der bisherigen Sicherheitsforschungspraxis zur Stärkung einer unmittelbaren Verwertung der Forschungsergebnisse. Wirksamer ist eine anwendungsorientierte Förderung von Sicherheitsinvestitionen.

Förderung schnellerer Zulassungs- und Zertifizierungsprozesse für IT-Sicherheitsprodukte, insbesondere wenn Behörden eine Genehmigungsfunktion ausüben. In diesem Fall sollten Wirtschaft und Behörden so früh wie möglich zusammenarbeiten, ohne komplexe Prozesse zu erzeugen.

Verbesserung der beruflichen Aus- und Weiterbildung in Bezug auf den sicheren Umgang mit digitalen Technologien und modernen Kommunikationsmitteln. Ein weiterer Schwerpunkt sollte die Bewusstseinssteigerung in Schulen sein, um so früh wie möglich den sicheren Umgang mit IT-Mitteln zu ermöglichen.

5.2. Beiträge der Industrie

Die Industrie leistet am besten im Rahmen von konkreten Projekten ihren Beitrag. Unspezifische Vorabentwicklungen sind aus wirtschaftlichen Gründen nicht machbar. Abbildbar ist, dass die Industrie geforderte Produkte rechtzeitig und gut liefert, wenn die Anforderungen eindeutig sind. Im Kern gilt, dass klare Marktanreize der Impuls für die Unternehmen sind.

Bereitschaft der Industrieunternehmen auf oberster Ebene:

- Informationssicherheit zur Chefsache zu machen,
- sich fortlaufend über die Sicherheitslage zu informieren,
- daraus abgeleitete Maßnahmen im Sinne der langfristigen Unternehmensentwicklung beharrlich umzusetzen,
- aktiv an der Erstellung von bewertbaren Lagebildern mitzuwirken.

Investitionen der Industrieunternehmen in die eigene Sicherheitsinfrastruktur durch technische, organisatorische sowie Weiterbildungsmaßnahmen.

Bereitstellung der Interoperabilität sowie Integrationsfähigkeit von Sicherheitstechnologien „Made in Germany“ in Lösungen nationaler und internationaler Betreiber sowie Hersteller.

Demonstration von Best-Practice-Beispielen, um die wirtschaftliche Umsetzung der Digitalen Souveränität überzeugend darzustellen.

Unterstützung der Umsetzung durch Teilnahme an Plattformen und Normungsgremien als konstruktiver Partner.

5.3. Beiträge der Politik

Fördern UND kaufen: Wahrnehmung der Vorbildfunktion des Staates bei Beschaffungsvorhaben. Setzen von hohen Sicherheitsanforderungen als wichtiges Vergabekriterium, das von allen Anbietern zu erfüllen ist.

Bewusster Einsatz von Sicherheitsreferenzprojekten in Heimatmärkten. Aufgrund ihrer Signalwirkung für ausländische Investoren dienen sie als zentrales Element der Wirtschafts- und Exportförderung über die gegenwärtige Messeunterstützung hinaus.

Entwicklung und kontinuierliche Fortschreibung von Forschungsroadmaps mit ausreichender Mittelausstattung und ihre konsequente Umsetzung in der Projektförderung.

Ausbau der FuE-Förderung und Beratungsprogramme für KMUs zur Verbesserung ihrer IT-Sicherheit.

Stärkeres Bewusstsein der Politik dafür, dass die IT-Sicherheitsbranche systemrelevant ist und Sicherheitskompetenz aus Deutschland und Europa zur Verfügung stehen muss.

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 851.000 Arbeitnehmer und weitere 690.000 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.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org