



# BDI

Bundesverband der  
Deutschen Industrie e.V.



## Grundsatzpapier Cybersicherheit


Voraussetzungen für die digitale Souveränität  
in Deutschland und Europa



# Inhaltsverzeichnis

---

<b>Vorwort</b> .....	<b>5</b>
<b>Einleitung</b> .....	<b>6</b>
<b>Digitale Souveränität -</b> Wettbewerbsfähigkeit des Wirtschaftsstandortes.....	<b>8</b>
<b>Digitale Souveränität -</b> Kompetenzen der Anwender.....	<b>12</b>
<b>Impressum</b> .....	<b>14</b>



**„Die Sicherheit und Vertrauenswürdigkeit von Daten ist ein strategischer Standortvorteil für Deutschland und Europa.“**

Dr. Hermann Rodler

## Vorwort

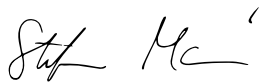
---

Die Industrie befindet sich inmitten des größten Transformationsprozesses der letzten Jahrzehnte. Die digitale Vernetzung von industriellen Prozessen, Fertigungsabläufen und gesamten Wertschöpfungsstrukturen schreitet mit enormer Dynamik voran. Ein Leben ohne digitale Informationstechnologien kann man sich heute kaum noch vorstellen. Dabei stehen wir erst am Anfang. Jüngste Studien prognostizieren, dass im Jahr 2020 über 20 Milliarden Dinge mit dem Internet verbunden sein werden.

In Deutschland und Europa legen wir besonderes Augenmerk auf die Digitalisierung industrieller Wertschöpfungsprozesse. Wir entwickeln intelligente vernetzte Maschinen, vernetzte Produktionsprozesse und versuchen, neue Geschäftsmodelle am Markt zu platzieren. In einigen Bereichen sind wir bereits heute Spitzenreiter. Insbesondere im Bereich der Cybersicherheit stehen deutsche und europäische Unternehmen ihren internationalen Konkurrenten in nichts nach. Dies ist von entscheidender Bedeutung.

Die digitale Transformation hängt vom Vertrauen der Anwender in die Sicherheit des Wirtschaftsstandortes ab. Unternehmen müssen ihre Daten – insbesondere wettbewerbs- und geschäftskritische Informationen – vor Ausspähung, Manipulation und Zerstörung schützen können. Dazu müssen Unternehmen Kompetenzen aufbauen, um Risiken bewerten und Lösungen entwickeln zu können. Dies ist keine einfache Aufgabe, doch eine notwendige, um die Wettbewerbsfähigkeit des europäischen Digitalisierungsstandortes zu stärken.

Mit dem vorliegenden Grundsatzpapier leistet die deutsche Industrie einen Beitrag in der Diskussion über die Cybersicherheit Europas. Ziel ist es, die digitale Souveränität zu stärken und den Austausch zwischen Unternehmen, Politik und Zivilgesellschaft weiterzuentwickeln. Cybersicherheit muss zu einem strategischen Standortvorteil werden. So erhöhen wir die Wertschätzung der Menschen für die Digitalisierung der Industrie.



**Dr. Stefan Mair**  
Mitglied der Hauptgeschäftsführung des BDI e.V.



**Dr. Hermann Rodler**  
Vorsitzender BDI-Ausschuss Digitale Wirtschaft,  
Telekommunikation und Medien



**Michael Ziesemer**  
Vorsitzender BDI-Ausschuss Digitale  
Wirtschaft, Telekommunikation und Medien



## Einleitung

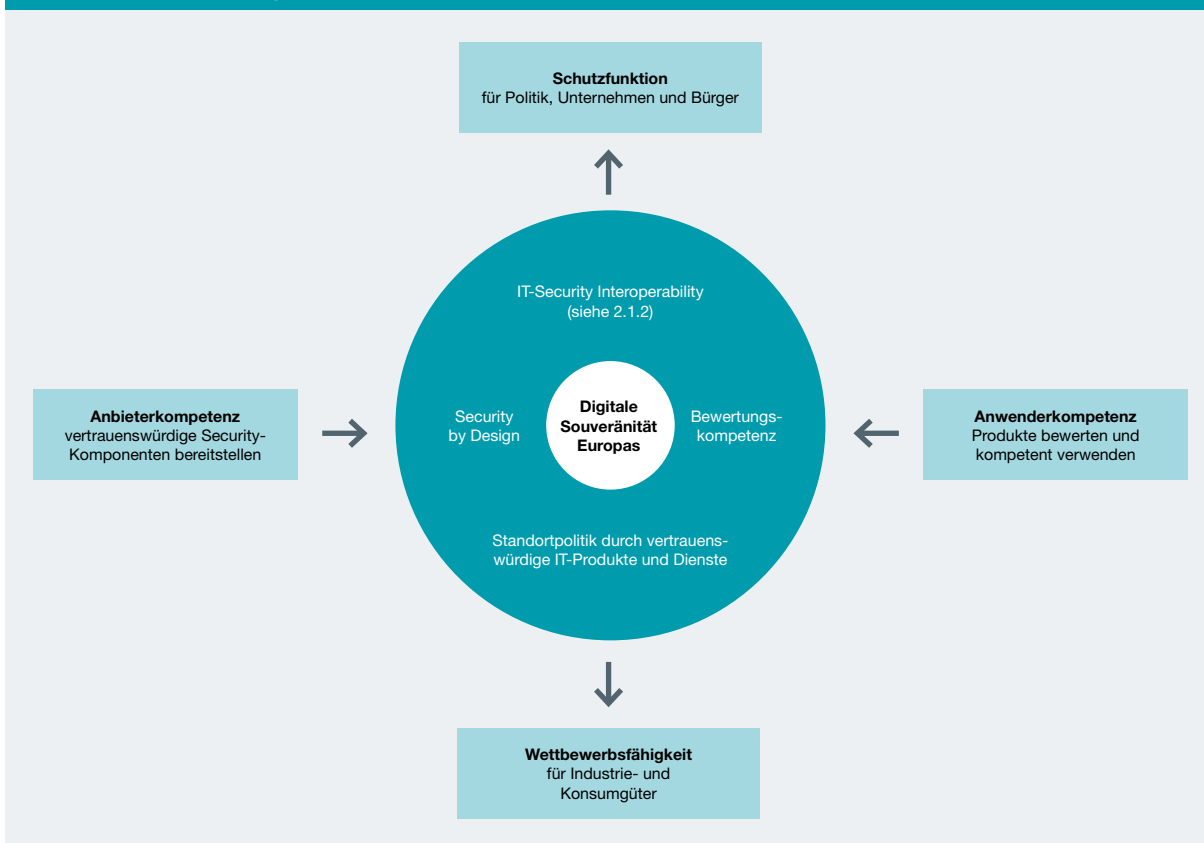
Die Integration digitaler Technologien entlang der gesamten Wertschöpfungskette schreitet mit enormer Dynamik voran. Politik und Wirtschaft haben es sich zum Ziel gesetzt, Deutschland zu einem Leitmarkt für die Digitalisierung von Industrieanwendungen zu entwickeln.

Der Sicherheit und Verfügbarkeit von Daten kommt eine strategische Bedeutung zu. Sie sind Voraussetzung für die Akzeptanz digitaler Lösungen im privaten wie auch im öffentlichen Leben. Wirtschaft und Politik müssen geeignete Rahmenbedingungen setzen, um die Übertragung, Speicherung und Nutzung von Daten in Europa besser gegen Ausspähung, Manipulation oder Zerstörung zu schützen. Nur mit der Stärkung der Cybersicherheit (d. h. IT-Security und Industrial Security) kann

die digitale Souveränität Europas ermöglicht und damit das Potential der Digitalisierung gehoben werden.

Die Cybersicherheit bietet zudem zusätzliche Markt- und Exportchancen für hiesige Unternehmen. Gelingt es, „Security by Design“ und Security in Echtzeit in Informations- und Kommunikationstechnologien (IKT), Industrie- und Konsumgüter zu integrieren, kann sich die europäische Industrie zum Leitanbieter der digitalen Wirtschaft entwickeln. Auf diese Weise bewahrt die Industrie Know-how, Technologieführung und Arbeitsplätze in Europa. Vertrauen in IKT-Infrastrukturen und -Anwendungen ist hierfür die Grundlage.

### Bestandteile der digitalen Souveränität



### Ausgangslage der Diskussion

Aufgrund der Dynamik der digitalen Transformation und den sich stetig wandelnden Herausforderungen wird hier auf eine abschließende Definition der digitalen Souveränität verzichtet.<sup>1</sup> Kern des hier diskutierten Verständnisses sind die drei Dimensionen: (1) Schutzfunktion, (2) Bewertungskompetenz und (3) Wettbewerbsfähigkeit.

#### Schutzfunktion:

Erst durch sichere und vertrauenswürdige IT-Produkte und -Dienstleistungen können Unternehmen, Bürger und staatliche Institutionen frei und selbstbestimmt im digitalen Raum agieren. Die Wahrung der Datenhoheit und die Verfügbarkeit einer sicheren IT-Infrastruktur sind zentrale Voraussetzungen. Nutzer müssen den Funktionen von Diensten und Infrastrukturen vertrauen können, d.h., dass keine Daten unbemerkt eingesehen, kopiert oder verändert werden können. So lange Unternehmen Verlust oder Manipulation ihrer Daten – insbesondere wettbewerbs- und geschäftskritische Informationen – befürchten müssen, werden sie sich nur sehr zurückhaltend oder nur in isolierten sicheren Räumen digitalisieren. Die digitale Souveränität stärkt das Vertrauen in digitale Wirtschaftsprozesse und trägt somit zum Gelingen der digitalen Transformation bei.

#### Bewertungskompetenz:

Die Analyse- und Bewertungskompetenz der Anwender ermöglicht einen souveränen Umgang mit Informationstechnologien. Anwender müssen die Sicherheit und Vertrauenswürdigkeit von Produkten und Anwendungen einschätzen und je nach Bedarf aus mehreren vertrauenswürdigen Technologie- und Handlungsoptionen auswählen können. Dies erfordert zugleich eine erweiterte Systemkompetenz der Anbieter. Sicherheitskomponenten sollten einfach und idealerweise über standardisierte Schnittstellen anwendbar bzw. austauschbar („easy to use“) sein. Die individuellen Schutzniveaus, beispielsweise für Kritische Infrastrukturen, für Industriegüter oder für die private Nutzung von IT-Systemen, müssen dabei berücksichtigt werden.

#### Wettbewerbsfähigkeit:

Mit der Stärkung der digitalen Souveränität wird zudem ein wettbewerbspolitisches Ziel verfolgt. Die Steigerung der IT-Kompetenz, d.h. die Fähigkeit, Schlüsseltechnologien im IKT-Bereich zu verstehen und zu entwickeln, gewinnt zunehmend an Bedeutung. Die europäische Industrie vertreibt Cybersicherheitsprodukte und -dienstleistungen bereits heute für den Weltmarkt und kooperiert dabei mit vertrauenswürdigen Zulieferern außerhalb Europas. Zugleich müssen Sicherheitslösungen aus Europa exporttauglich für den Weltmarkt sein. Dabei gilt für den heimischen Markt: Vertrauen in die Sicherheit bzw. Integrität und Authentizität von Daten ist ein strategischer Standortvorteil.

<sup>1</sup> Vgl.: BITKOM, Digitale Souveränität Positionsbestimmung und erste Handlungsempfehlungen für Deutschland und Europa, Berlin 2015, eingesehen auf: [https://www.bitkom.org/Publikationen/2015/Positionspapiere/Digitale-Souveraenitaet/BITKOM-Position\\_Digitale\\_Souveraenitaet.pdf](https://www.bitkom.org/Publikationen/2015/Positionspapiere/Digitale-Souveraenitaet/BITKOM-Position_Digitale_Souveraenitaet.pdf), am 10.04.2016 oder ZVEI, Digitale Souveränität, Debatte über einen besonnen Umgang mit internationalen Herausforderungen und die Stärkung des Industriestandorts Deutschland, Diskussionspapier, Berlin 2015, eingesehen auf: <http://www.zvei.org/Publikationen/ZVEI-Diskussionspapier-Digitale-Souveraenitaet.pdf>, am 10.04.2016.

## Digitale Souveränität – Wettbewerbsfähigkeit des Wirtschaftsstandortes

Digitale Souveränität bedeutet Standortpolitik. Damit Anwender selbstbestimmt aus vertrauenswürdigen Produkt- und Handlungsoptionen auswählen können, müssen diese wettbewerbsfähig und langfristig auf dem Markt angeboten werden. Dies gilt sowohl für die Cybersicherheitswirtschaft als auch für alle anderen Bereiche der Digitalisierung.

Bei der Herstellung von Industrie- und Konsumgütern im IKT-Bereich muss die Sicherheit verstärkt im Produktdesign sowie im Produktionsprozess mitgedacht werden. Sie muss als Teil der Produktentwicklung, Qualitätsprüfung sowie -dokumentation verstanden werden. Das Motto muss lauten: „Security by Design“.

Die Cybersicherheit ist ein zukunftsweisender Wachstumsmarkt. Die Stärken der deutschen IT-Sicherheitsindustrie liegen im Bereich der Dienstleistungen und der Hochsicherheit<sup>2</sup>. Zudem ist Deutschland führend in der Entwicklung von Unternehmenssoftware und eingebetteten Systemen. Auch im Bereich der Halbleiterindustrie setzt die europäische Industrie weltweit Maßstäbe. Trotzdem gehört Europas Industrie nicht zu den Spitzenstandorten der digitalen Wirtschaft.

Für den globalen Erfolg der europäischen Wirtschaft ist es wichtig, ein global akzeptiertes Rahmenwerk für die Sicherheit und Privatheit von Daten in der hypervernetzten Welt zu schaffen – unter Einbezug der europäischen Datenschutzregulierung und der Network-Information-Security Richtlinie. Nur wenn langfristig Verlass auf die Verfügbarkeit, Innovationsfähigkeit und Wettbewerbsfähigkeit von Cybersicherheitsprodukten ist, fragen Anwender Sicherheitslösungen aus Deutschland und Europa nach. Die Stärkung und Förderung dieser Kompetenzen muss ein strategisches Ziel europäischer Wirtschafts- und Standortpolitik sein.

### Was es zu tun gilt

#### Fachkräfte gezielt ausbilden

Die Verfügbarkeit hochausgebildeter Fachkräfte ist eine zentrale Voraussetzung für die Innovations- und Wettbewerbsfähigkeit Deutschlands. Der schon jetzt augenscheinliche Fachkräftemangel wird zu einem zunehmenden Problem für den Wirtschaftsstandort. Dies gilt insbesondere für den Bereich der Cybersicherheit. Die von den deutschen Unternehmen dringend benötigten

Experten sind heute am Markt kaum verfügbar. Die Rekrutierung von Experten aus anderen Ländern ist vielfach mit Risiken bzgl. der Vertrauenswürdigkeit verbunden.

Bund und Länder sind nachdrücklich aufgefordert, eine gemeinsame Aus- und Weiterbildungsagenda, insbesondere im Bereich der IT-Kompetenzen aufzustellen und umzusetzen. Im Zuge der Verschmelzung digitaler und physikalischer Welt sind methodische und konzeptionelle Kompetenzen im Querschnitt aus Mathematik, Technologie/Technik, Sensorik, Digitale Medien, Naturwissenschaft und Ingenieurwesen relevant. Darüber hinaus muss Kreativität und Erfindergeist in den Schulen gefördert werden. Der Beschluss der Kultusministerkonferenz, die Digitalisierung neben Rechnen, Lesen und Schreiben als vierte Kulturtechnik zu verstehen, wird ausdrücklich begrüßt.

Vor diesem Hintergrund müssen bereits heute die Weichen richtig gestellt werden: Über die Schaffung neuer Ausbildungsgänge zum Cybersicherheits-Experten, die Einrichtung entsprechender universitärer Lehrstühle und Schwerpunkt-Cluster, bis hin zu einer intensivierten Forschungsförderung im Bereich der Cybersicherheit. Dies umfasst auch die Bereitstellung entsprechender Budgets.

In Deutschland existiert bereits heute eine leistungsfähige Forschungs- und Innovationslandschaft, die sich aus Universitäten, Forschungs- und Entwicklungseinrichtungen, großen und mittelständischen Unternehmen sowie Start-ups zusammensetzt. Diese Innovationskultur muss weiterhin gestärkt und gefördert werden.

#### Industrielle Gründerkultur stärken

Um im globalen Wettbewerb bestehen zu können, bedarf es guter Ideen und Unternehmen, die aus Ideen Umsatz generieren. Dies trägt entscheidend zur Innovations- und Entwicklungsfähigkeit des Wirtschaftsstandortes bei.

Digitale Innovationen entwickeln ihr Potential zumeist außerhalb bestehender Geschäftsstrukturen. So werden nach aktuellen Studien bis zu 50 Prozent aller IoT-Geräte in den kommenden Jahren von Start-ups entwickelt.<sup>3</sup> Bei der Zahl von Start-ups liegt Deutschland

<sup>2</sup> Vgl.: Bundesministerium für Wirtschaft und Energie: Der IT-Sicherheitsmarkt in Deutschland, Berlin 2014.

<sup>3</sup> Vgl.: Gartner Says By 2017, 50 Percent of Internet of Things Solutions Will Originate in Startups That Are Less Than Three Years Old, eingesehen auf <http://www.gartner.com/newsroom/id/2869521>, am 24.06.2016.



lediglich im internationalen Mittelfeld. Die Zahl der Existenzgründungen war im Jahr 2015 sogar rückläufig (-17 %).<sup>4</sup>

Es bedarf der Förderung einer dynamischen Start-up-Kultur, die Trial-and-Error Prozesse ermöglicht und dabei das Thema Cybersicherheit in den Fokus rückt. Start-ups und etablierten Unternehmen muss ein gemeinsamer Entwicklungsdialog ermöglicht werden. Die Politik ist aufgefordert, die Rahmensetzung für Wagnis- und Beteiligungskapital in der Forschungsförderung und der Rechts- und Steuerpolitik anzupassen.

#### Finanzielle Anreize für Innovationen schaffen

Zur Förderung der Cybersicherheit, insbesondere in kleinen und mittelständischen Betrieben, bedarf es eines geeigneten Anreizsystems für Innovationen. Investitionen in immaterielle Vermögenswerte, wie beispielsweise in Ausbildung, Entwicklung und Prozessinnovation, werden in einem anlageorientierten Investitionsbegriff nicht ausreichend berücksichtigt. Immaterielle Investitionen verändern die Anforderungen an Kreditsicherheiten, deren Fungibilität sowie juristische Durchsetzbarkeit. Zudem sind diese Vermögenswerte schwerer zu bewerten (bspw. Patente oder Know-how sind immer abhängig von spezifischen Geschäftsmodellen). Es müssen sich im Zusammenspiel von Industrie und Banken neue Besicherungsstandards und Bewertungsansätze etablieren, die den Besonderheiten des digitalen Strukturwandels in allen Branchen Rechnung tragen. Die steuerliche Forschungsförderung stellt ein geeignetes Instrument dar, um in Unternehmen aller Größen die notwendigen Innovationen zur Digitalisierung gezielt zu flankieren. Deutschland sollte die in vielen Industriestaaten bewährte steuerliche Forschungsförderung einführen.

Zudem wird die Beteiligung Deutschlands an der European Cybersecurity Organization (ECISO) und der damit verbundenen cPPP (contractual public private partnership) begrüßt. Die Entwicklung an dem von der Europäischen Kommission geforderten „labelling scheme for the security of ICT products“ (EU Trust Label) wird von der deutschen Industrie begleitet.<sup>5</sup>

#### Wichtige Rolle der öffentlichen Beschaffung

Der europäische Cybersicherheitsmarkt ist ein strategisch bedeutsamer Wirtschaftssektor. Der öffentlichen Hand fällt daher eine besondere Verantwortung in der eigenen Beschaffung zu. Unternehmen benötigen Aufträge und Referenzprojekte der öffentlichen Stellen in Europa, um ein kritisches Marktvolumen generieren zu können. Staatliche Beschaffungsentscheidungen werden in der Öffentlichkeit auch als Vertrauensiegel verstanden. Eine gleichbleibende Qualität eines Sicherheitsproduktes oder einer -dienstleistung muss über den gesamten Lebenszyklus hinweg gewährleistet werden und beim Auswahlprozess eine entsprechend stärkere Berücksichtigung finden.

International anerkannte Sicherheitsstandards können bei der Auswahl hilfreich sein und tragen zu einer breiteren Verwendung von Sicherheitsprodukten bei. Dies gewährleistet, dass wettbewerbsfähige europäische Anbieter vertrauenswürdige, konkurrenzfähige Produkte anbieten können. Zudem würden die fragmentierten europäischen Einzelmärkte zu einer konvergenteren Nachfragepolitik kommen.

Für den überwiegenden Teil des Cybersicherheitsmarktes führen nationale Standards zu Marktabschottung und verhindern somit die internationale Ausrichtung der Branche. Ziel muss sein, dass ein einheitlicher europäischer Cybersicherheitsmarkt dazu beiträgt, dass auch internationale Standards ein entsprechend hohes Sicherheitsniveau gewährleisten. Im Nischenbereich, bspw. im Hochsicherheits-Marktsegment, können nationale Standards durchaus sinnvoll und notwendig sein. Gerade hier besitzen deutsche Unternehmen eine hohe Kompetenz.

#### Zugang zu den Weltmärkten verbessern

Zur Stärkung der internationalen Wettbewerbsfähigkeit, muss der Cybersicherheitsbranche der Zugang zu den Weltmärkten gewährleistet werden. Insbesondere bei der Exportkontrolle darf es nicht zu einer einseitigen Benachteiligung europäischer Cybersicherheitsunternehmen kommen. Mit der anstehenden Dual-Use-Reform droht jedoch ein Nadelöhr im Export zu entstehen.

Der beabsichtigte *human security approach* soll dem stärkeren Schutz von Menschenrechten dienen. Dieses Ziel wird vom BDI unterstützt. Unspezifische Regeln, wie sie derzeit angedacht sind, schaffen jedoch keine Rechts- und Planungssicherheit. Europäische

<sup>4</sup> KfW Bankengruppe: KfW-Gründungsmonitor 2016, Frankfurt am Main 2016, S.1.

<sup>5</sup> Strengthening Europe's Cyber Resilience System and Fostering a Competitive and Innovative Cybersecurity Industry (05/07/2016), eingesehen auf: [http://ec.europa.eu/newsroom/dae/document.cfm?doc\\_id=16546](http://ec.europa.eu/newsroom/dae/document.cfm?doc_id=16546), am 15.07.2016.

Unternehmen können Lieferzusagen hierdurch wesentlich schwerer einhalten, als ihre internationale Konkurrenz. Dies führt zu einem nachhaltigen Wettbewerbsnachteil für die europäische Cybersicherheitsbranche, jedoch nicht zu einem stärkeren Schutz von Menschenrechten. Dies muss auf anderem Wege erreicht werden. Der BDI schlägt für die Dual-Use-Reform Regelungsalternativen vor, die anhand von Produkt- und Länderlisten kritische Güter und Länder benennen. Dies macht die Exportkontrolle auch im Unternehmensalltag handhabbar.

Innerhalb der EU wird zum Teil eine unterschiedliche Effizienz, Schnelligkeit und Prüftiefe der Exportkontrolle – insbesondere im Bereich Dual Use – praktiziert. Dies schadet Unternehmen, die jenseits der Nische nur dann wachsen können, wenn sie sich auf den Export konzentrieren. Dies gilt nicht nur für die erste Ausfuhr von Sicherheitsprodukten und -komponenten. Auch die Nachsendung derartiger Produkte ins Ausland, bspw. im Zuge von Wartungen und Upgrades, muss leicht und ohne Exporteinschränkungen möglich sein.

### IT-Security Interoperability ermöglichen

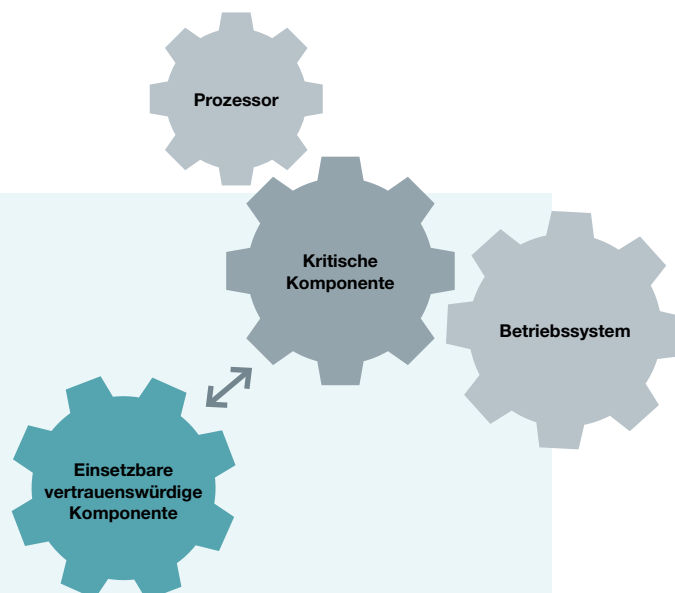
Sicherheit muss als Teil der Produktentwicklung, Qualitätsprüfung sowie -dokumentation verstanden werden. Die Möglichkeit der Erweiterung oder des Austausches der IT-Sicherheitskomponenten sollte jedoch grundsätzlich bestehen. Ein vollständiger Austausch und Ersatz stellt im Regelfall keine reale Option dar. Im Umkehrschluss ist der Austausch von unsicher eingeschätzten Komponenten oder der Einbau von vertrauenswürdigen und kontrollierbaren Komponenten erforderlich.

Die notwendigen Schnittstellen sowie die Austauschbarkeit der einzelnen Komponenten sollten vom Hersteller der Kommunikationsinfrastrukturen und IKT-Anwendungen ermöglicht werden. Dies erhöht die Sicherheit und schafft mehr Anwendungsfälle, für Geschäftsmodelle und Vorgänge, die ohne Sicherheitsfunktionen zunächst nicht möglich waren (bspw. besserer Service durch gesicherte Fernwartungszugänge; Verwendung von Cloud-Diensten durch eine Ende-zu-Ende-Verschlüsselung). Letztendlich stärkt eine derartige Austauschbarkeit die Exportchancen und Marktzugänge der europäischen Industrieunternehmen.

Politik und Wirtschaft müssen in einen gemeinsamen Dialog zum Thema „IT-Security Interoperability“ mit internationalen Herstellern von

Kommunikationsinfrastrukturen treten. Solch ein „Schnittstellendialog“ sollte auf Basis konkreter Beispiele und Anliegen geführt werden. Technische Möglichkeiten, Bedarfe und potenzielle Anwendungsbeispiele sollten aus Anbieter- und Anwendersicht artikuliert werden.

Die Industrie wird sich hierzu entsprechend vorbereiten und diesen Input in gemeinsamen Workshops mit allen Beteiligten abfragen und als Vorbereitung des „Schnittstellendialogs“ verwenden. Ziel ist eine gemeinsame Gesamtlösung, die kontinuierliche Verbesserung der Schutzmöglichkeiten für Bürger, Unternehmen und Behörden verspricht. Die Industrie begrüßt hierfür die Unterstützung der Politik, um die Führungsrolle der in Europa tätigen Industrie weiter zu stärken und auszubauen.







**„Sicherheit muss über die gesamte Wertschöpfungskette gewährleistet werden. Die Möglichkeit der Erweiterung oder des Austausches der IT-Sicherheitskomponenten sollte jedoch grundsätzlich bestehen.“**

Michael Ziesemer

## Digitale Souveränität - Kompetenzen der Anwender

Die Sicherheit von digitalen Ökosystemen ist aufgrund der breiten gesellschaftlichen Vernetzung eine zunehmend öffentliche Herausforderung. Individuelles Fehlverhalten kann direkte Auswirkungen auf Vermögen, Handlungsfähigkeit und gegebenenfalls Gesundheit anderer Nutzer haben. Die Sicherheit im Cyberraum muss daher als eine gesellschaftliche Aufgabe verstanden werden.

Im Business-to-Business-Bereich sind vertrauenswürdige und sichere IT-Lösungen eine unerlässliche Voraussetzung für Produkte und Dienste. Jedoch findet auch im Business-to-Customer-Bereich zunehmend ein Umdenken statt. Bereits heute werden sicherheitsrelevante Eigenschaften oder Verfahren eines Produktes oder Dienstes vom Hersteller veröffentlicht, da dies für Kunden ein Qualitätskriterium und damit ein Kaufargument ist. Damit Anwender Schutz- und Qualitätsniveaus bewerten können, müssen Informationen bzw. Eigenschaften des Produktes oder Dienstes auf verständliche Art und Weise dargestellt werden. Dies kann auch durch Dritte, in Form eines Labels mit entsprechender Marktdurchdringung, gewährleistet werden.

Die Herausforderungen der Cybersicherheit unterliegen ständiger Veränderungen. Angriffsmöglichkeiten und technische Schwachstellen ändern sich stetig und können daher niemals statisch als Produkt eingekauft werden. Dies belegen auch derzeit genutzte Angriffsvektoren, die nicht eingesetzte kryptografische Verfahren brechen, sondern Schwachstellen in der Implementierung der Einsatzumgebung finden. Prüfzertifikate und Labels müssen diesem Umstand Rechnung tragen.

Insbesondere institutionelle Anwender müssen Sicherheitsmaßnahmen gut implementieren und stets im Betrieb die notwendige Nachsorge treffen. Die Sicherheit von Informationstechnologien muss dabei als fortlaufender Prozess verstanden werden.

### Was es zu tun gilt

#### Neutrale Prüfstellen einrichten und Verfahren dynamisieren

Um die Bewertungskompetenz institutioneller Anwender zu steigern, bedarf es neutraler Prüfstellen und vertrauenswürdiger bzw. einheitlicher Labels. Dabei müssen die Angriffs- und Manipulationssicherheit des Produktes, dessen Produktionsstätte sowie die jeweiligen

Produktionsabläufe überprüft werden können. Insbesondere für sicherheitskritische Bereiche oder Spezialanwendungen im B2B-Bereich ist dies wichtig. Die Prüfstellen müssen daher eine tiefere Prüfung des Sicherheitsniveaus für Soft- und Hardware nach allgemein anerkannten state-of-the-art-Zertifizierungsprozeduren, wie CCRA<sup>6</sup> oder SOG-IS MRA vornehmen können. Die Forschung für geeignete Testverfahren und die Darstellung der Sicherheitsbewertung, bspw. über eine Metrik, leistet hierfür wertvolle Unterstützung.

Die Verfahren dürfen keine Markthindernisse darstellen. Die Erfahrung zeigt, dass bereits bestehende Prüfverfahren kosten- und zeitintensiv sind. Sie müssen vielmehr innovationsfördernd wirken, das heißt Marktzyklen müssen berücksichtigt und zeitnahe Markteintritte ermöglicht werden. Hierfür ist ein gestuftes Vorgehen wichtig, das heißt Basisprüfungen für Konsumgüter und tiefergreifende Nachweise für sicherheitskritische Bereiche. Vereinheitlichte und international akzeptierte Prüfprozesse und ein für alle Beteiligten gültiges politisches Regelwerk müssen diese Kosten auf ein Mindestmaß reduzieren.

Zudem gewährleistet die Neutralität staatlicher Prüfstellen ein hohes Sicherheitsniveau der dort zertifizierten Produkte. Die Schaffung von Institutionen im gleichen Verantwortungsbereich zur Schwächung dieser Sicherheitsmechanismen (bspw. im Bereich Kryptographie) darf daher keine Option sein.

#### Internationalen Rechtsrahmen stärken

Die Schaffung eines international vergleichbaren Rechtsrahmens ist, insbesondere vor dem Hintergrund einer global agierenden IT-Branche, von besonderer Bedeutung. Dabei müssen gemeinsame, internationale Maßstäbe für den staatlichen Zugriff auf Kommunikations- und Informationsstrukturen entwickelt werden. Aufbauend auf dem globalen Internet Governance Prozess der UN (bspw. im Internet Governance Forum oder NETmundial) gilt es, auch im Bereich der internationalen Cybersicherheit, globale Verfahren und Foren zu entwickeln.

<sup>6</sup> Participating parties of CCRA, the Common Criteria Recognition Arrangement, mutually recognise intermediate levels of evaluation against the Common Criteria (CC) standard. CC is the predominant ISO-standard for IT security, and the certificates are accepted both for commercial and public domain applications, as well as for essential services.

Die deutsche Industrie begrüßt die Cyber-Außen und -sicherheitspolitik der Bundesregierung in den Vereinten Nationen und der OECD. Deutschland muss seiner Tradition als Zivilmacht auch in Fragen der internationalen Cybersicherheit gerecht werden. Die Schaffung eines freien und sicheren digitalen Raums kann allerdings nur durch starke Allianzen auf europäischer Ebene erreicht werden. Politik und Industrie sind gleichermaßen aufgefordert, sich für die Schaffung eines organisierten international sicheren Rechtsrahmens einzusetzen.

#### Awareness für Cybersicherheit steigern

Fast die Hälfte der Sicherheitsvorfälle sind auf Nachlässigkeit oder Fehlverhalten der Nutzer zurückzuführen.<sup>7</sup> Die Stärkung der digitalen Kompetenzen, bereits durch Bildungsmaßnahmen in Schulen und Universitäten, trägt signifikant zur Sicherung des Industriestandorts

Europa bei. Die Sensibilisierung der Öffentlichkeit für die Bedeutung der Cybersicherheit muss von Unternehmen und der Politik gleichermaßen vorangetrieben werden. Die Politik muss weiterhin die Cybersicherheit als Voraussetzung für den Erfolg der Digitalisierung verstehen und kommunizieren.

Die Zusammenarbeit von Wirtschaft und Politik in cybersicherheitspolitischen Initiativen, wie der Allianz für Cyber-Sicherheit ist wichtig. Der übergreifende Charakter muss sich auch in der Zusammenarbeit der Behörden und Ministerien widerspiegeln. Kein Arbeitsbereich kann ohne den anderen die Ziele sinnvoll voranbringen. Die Politik ist aufgefordert, die gegenseitige Informierung und Abstimmung zwischen den verantwortlichen Ministerien sicherzustellen.

<sup>7</sup> Vgl.: IDC: Mobile Security in Deutschland 2015, Frankfurt am Main 2015.



## Impressum

---

### Herausgeber

Bundesverband der Deutschen Industrie e.V. (BDI)  
Breite Straße 29  
10178 Berlin  
T: +49 30 2028-0  
[www.bdi.eu](http://www.bdi.eu)

### Redaktion

Iris Plöger, Abteilungsleiterin  
Abteilung Digitalisierung, Innovation und Gesundheitswirtschaft

Quirin Blendl, Referent  
Abteilung Digitalisierung, Innovation und Gesundheitswirtschaft

### Konzeption & Umsetzung

Sarah Pöhlmann, Referentin  
Abteilung Marketing, Online und Veranstaltungen

### Layout

Tilman Schmolke  
[www.europrint-medien.de](http://www.europrint-medien.de)

### Druck

Das Druckteam Berlin  
[www.druckteam-berlin.de](http://www.druckteam-berlin.de)

### Verlag

Industrie-Förderung GmbH, Berlin

### Bildnachweis

Cover: © 116954535 / maxim / Fotolia.com  
Seite 4: © 89345883 / Julien Eichinger / Fotolia.com  
Seite 11: © 06250578 / vege / Fotolia.com

### Stand

August 2016  
BDI-Publikations-Nr. 0050



