Bundesverband IT-Sicherheit e.V.

Secure Platform

"Digitale Souveränität als Motivation für ein sicheres IT-Ökosystem in Deutschland und Europa"

TeleTrusT-Positionspapier

2020

Danksagung

Diese Publikation wurde im TeleTrusT-Arbeitskreis "Secure Platform", einem Untergremium der TeleTrusT-AG "Recht", erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Dr. André Kudra, esatus, Leiter der TeleTrusT-AG "Blockchain" und Leiter des TeleTrusT-AK "Secure Platform"

Autorenliste (Auszug)

Adolf, Alexander - Condition-ALPHA
Aigner, Alexander - FH Hagenberg (Oberösterreich)
Barchnicki, Sebastian - secunet
Heyde, Steffen - secunet
Kudra, André - esatus
Mutz, Reinhard - World Privacy and Identity Association
Olfert, Sarah - esatus
Rieblinger, Philipp - esatus
Rieken, Ralf - Uniscon

Redaktion

Abou Nasser, Morad - Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Mühlbauer, Holger - Bundesverband IT-Sicherheit e.V. (TeleTrusT)

In dieser Publikation werden zahlreiche Anglizismen verwendet, da sie sich in der zugrundeliegenden Fachdiskussion branchentypisch verfestigt haben.

Impressum

Herausgeber:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
Fax: +49 30 400 54 311
E-Mail: info@teletrust.de
https://www.teletrust.de

Inhalt

1 Überblick

Informationstechnik (IT) ist fest in jedem Bereich des Alltags verankert und Grundlage der Digitalisierung. "Digitale Souveränität" ist eine entscheidende Vorbedingung für die Wettbewerbsfähigkeit Europas, gerade auch mit Blick auf "Industrie 4.0", aber ebenso für den Betrieb kritischer Infrastrukturen (KRITIS) oder Vorhaben wie GAIA-X [1] und 5G.

Derzeit ist diese Digitale Souveränität aus mehreren Gründen nicht gegeben:

1. Es bestehen starke Abhängigkeiten von auswärtigen Technologieproduzenten.
2. Eingesetzte Technologien sind komplexe, intransparente Systeme.
3. Nachhaltige IT-Sicherheit scheint kein Entscheidungskriterium zu sein.

In der Diskussion mit Anwendern zeigt sich, dass eine Resignation einsetzt und die eigenen Anforderungen an das bestehende Angebot - im Regelfall von marktdominierenden US-Lösungsanbietern - angepasst werden, anstatt umgekehrt. Aufgrund der Bedeutung für die wirtschaftliche Wettbewerbsfähigkeit und Zukunft Europas ist das Sich-Abfinden mit dem Status Quo keine akzeptable Option. Auch das Auditieren bestehender Systemlösungen ist aufgrund der inhärenten Komplexität wenig zielführend und nicht ausreichend.

Es ist weder realistisch, notwendig noch wünschenswert, alle Elemente einer digitalen Infrastruktur von europäischen Herstellern entwickeln und fertigen lassen zu wollen. Eine erfolgversprechende und zielführende Strategie ist jedoch, ausgewählte Themenfelder durch europäische Anbieter zu besetzen. Die Wiedererlangung Digitaler Souveränität kann erreicht werden durch:

- Reduktion digitaler Abhängigkeit von außereuropäischen Anbietern,
- Abkehr von schädlichen Designparadigmen.

sowie

- Begünstigung eines verantwortungsbewussteren Käuferverhaltens.

Dieses Positionspapier ist ein Aufruf des TeleTrusT-Arbeitskreises "Secure Platform", mit Handlungsempfehlungen gerichtet an die maßgeblichen Akteure, die für eine neue Digitale Souveränität sorgen können:

- Politik mit Vorbildfunktion und regulatorischer Kompetenz
  - o Regelungsrahmen, Vorbildfunktion und staatliche Beschaffung
  - o Förderprogramme IT-Sicherheit
  - o Eigeninitiative des Bundes
  - o Zulassung und Zertifizierung
  - o Begleitung und Förderung des Standardisierungsprozesses

- Industrie und Dienstleister als Käufer und Anwender von Technologien
  - o Eigene Bewertungskompetenz stärken
  - o Eigene Compliance stärken und Haftungsrisiken reduzieren
  - o Eigene Kompetenz zur Systemintegration auf- bzw. ausbauen und auf EU-weite, standardisierte Zertifizierungen setzen

- Hersteller von IT- und IT-Sicherheits-Produkten
  - o Engagement in der technischen Standardisierung zur Umsetzung eines EU-weiten Zertifizierungssystems
  - o Bereitstellen sicherer Produkte
  - o Informations- und Aufklärungsangebote schaffen und ausbauen

Ein weiterer Schwerpunkt des Arbeitskreises ist die Erarbeitung einer technischen, architekturellen Empfehlung für sichere Plattformen, die für die Ausgestaltung von z.B. KRITIS-Kernkomponenten und GAIA-X-Knoten angewendet werden sollte. Konkrete Zielvorstellung des Arbeitskreises ist die Referenzimplementierung einer "Secure Platform" für hohe und höchste Sicherheitsstufen im GAIA-X-System oder bei KRITIS-Kernkomponenten. Eine derartige Referenzimplementierung einer "Secure Platform" ist als Grundlage der Digitalen Souveränität anzusehen, so dass eine entsprechende vorwettbewerbliche Förderung zur Reduktion technologischer Risiken notwendig erscheint.

2 Digitale Souveränität: Status quo

Die Digitalisierung schreitet mit enormer Dynamik voran und verankert Informationstechnik in jedem Bereich des Alltags. Sie ist Treiber und Basis für das Wohlergehen unserer Gesellschaft, doch sie schafft auch eine massive Abhängigkeit. Ob bei der täglichen Arbeit, dem Medienkonsum in der Freizeit, dem Betrieb Kritischer Infrastrukturen, GAIA-X-Knoten oder 5G-Routern, nichts geht ohne IT. Die im Betriebskontext oft geforderte "Digitale Souveränität" ist aktuell eine illusorische Vorstellung, da - wie nachfolgend ausgeführt - Abhängigkeiten von nicht kontrollierbaren Faktoren entstanden sind.

Abhängigkeit von externer Technologieproduktion und -lieferung: Europäischen Unternehmen kommt als Lieferanten für breit eingesetzte IT kaum mehr eine Rolle zu. Die marktführenden Technologien werden in fast allen Bereichen außerhalb Europas gefertigt, dominierend sind Asien und die USA. Hersteller sind an die jeweiligen gesetzlichen Vorgaben und kulturellen Denkweisen ihres Landes gebunden. So unterscheiden sich die Einschätzungen zur Stärke einzusetzender Verschlüsselung oder bewusster Integration von "Back Doors" im weltweiten Vergleich sehr stark. Eine vollständige Vertrauenswürdigkeit kann mit solchen Komponenten nicht gewährleistet werden, mangels Alternativen sind sie jedoch überall im Einsatz.

Eingesetzte Technologien sind komplexe "Black Boxes": Aktuelle IT-Systeme sind vielschichtige Gebilde aus Hard- und Software, deren Komplexität selbst für Experten oft schwer durchdringbar ist. Zudem sind technische Eigenschaften auf Detailebene und Programmcodes nicht für eine eigenständige bzw. unabhängige Prüfung verfügbar ("Closed Source"). Es ist nicht feststellbar, ob ein Produkt lediglich die gewünschten Funktionalitäten bereitstellt oder ob Schwachstellen und versteckte "Back Doors" für Manipulationen vorhanden sind. Diese können sich praktisch auf jeder Ebene des IT-Systems befinden, auch in der Hardware, den verbauten "Chips". Eine potentielle Schwachstellensuche gleicht der sprichwörtlichen Suche nach der Nadel im Heuhaufen, ohne jedoch zu wissen, wie die Nadel aussieht. Und selbst wenn eine solche identifiziert wird, kann nicht garantiert werden, dass jedes Gerät einer Serie in Hard- und Software exakt identisch ist.

Nachhaltige IT-Sicherheit ist kein maßgebliches Kriterium für Design und Erwerb: Design und Produktion aktueller Systeme sind durch die Paradigmen "maximale Funktionalität" und "geringe Time-to-Market" geprägt. Ist das Produkt erst einmal auf dem Markt, werden sicherheitsrelevante Updates vernachlässigt. Auf Käuferseite werden Vertrauenswürdigkeit und Sicherheit von IT fälschlicherweise als Selbstverständlichkeit angesehen. Systeme mit nachweislich höherem Sicherheitsniveau erlangen keine Anwenderaufmerksamkeit, da niedrige Preise und Bequemlichkeit schlagende Kaufkriterien sind. Dass IT-Sicherheit kein Design- und Langfristziel ist, zeigt die steigende Zahl von IT-Sicherheitsvorfällen (vgl. BSI-Lagebilder[2]). Als Konsequenz sind das allgemeine Sicherheitsniveau und die Vertrauenswürdigkeit aktuell verbreiteter Systeme deren gesellschaftlicher Bedeutung nicht angemessen.

Erhebliche Risiken erwachsen dadurch bei architektureller Ausgestaltung und Betrieb von (nicht nur kritischen) Infrastrukturen, die zudem meist EU- bzw. europaweit vernetzt sind. Eine Betriebsunterbrechung oder Kompromittierung einer einzelnen Komponente kann so systemische Konsequenzen haben, die im Extremfall den temporären Ausfall vollständiger Wirtschaftszweige bewirken. Ein Weg aus der unsouveränen Position bedeutet zwangsläufig die

1. Reduktion digitaler Abhängigkeit von außereuropäischen Anbietern
2. Abkehr von schädlichen Designparadigmen, sowie
3. Begünstigung eines verantwortungsbewussteren Käuferverhaltens.

Die unmittelbaren Folgen sind ein höheres Sicherheitsniveau und gestärkte Vertrauenswürdigkeit eingesetzter Komponenten und mittelbar die Wiedererlangung Digitaler Souveränität. Die Voraussetzungen dafür sind in Deutschland und Europa aussichtsreich: Vorhandene Technologieproduktionen könnten ausgebaut und Anreize für den Einsatz sicherer Systeme geschaffen werden. Auch regulatorisch, denn Europa steht aufgrund des "Exportschlagers" EU-DSGVO im Fokus der Weltöffentlichkeit und könnte für sichere Systeme einen weiteren Leuchtturm etablieren. Deutsche Hersteller und Forschungsinstitute der IT-Sicherheit behaupten sich durch umfassende Fachexpertise, Kompetenz und Erfahrung, sie genießen internationales Vertrauen und Ansehen.

Dieses Positionspapier ist ein Aufruf des TeleTrusT-Arbeitskreises "Secure Platform" mit Handlungsempfehlungen, gerichtet an die maßgeblichen Akteure, die für eine neue Digitale Souveränität sorgen können:

1. Politik als Inhaber einer Vorbildfunktion und regulatorischer Kompetenz
2. Industrie und Dienstleister als Käufer und Anwender von Technologien
3. Hersteller von IT- und IT-Sicherheitsprodukten

Der TeleTrusT-Arbeitskreis hat sich als weitere Zielsetzung die Erarbeitung einer technischen, architekturellen Empfehlung für sichere Plattformen gegeben, die als Grundlage für die Ausgestaltung von z.B. KRITIS-Kernkomponenten und GAIA-X-Knoten angewendet werden sollte. Dies wird sich an eine technisch versierte Zielgruppe richten, die Gestaltungs- und Entscheidungskompetenz besitzt sowie das Bestreben, in ihrem jeweiligen Wirkungsbereich sichere Systeme zu etablieren bzw. zu betreiben.

3 Digitale Souveränität als gesamtgesellschaftliche Zielsetzung

Digitale Souveränität bedeutet, dass Deutschland und die EU die wesentlichen Werte von Bürgern, Behörden und Wirtschaft technisch eigenständig schützen können. Dies umfasst:

- Private und Berufs-, Staats- und Geschäftsgeheimnisse
- Datenschutzkonformität
- Kartellrechtskonformität
- Vertrauen und Reputation
- Finanzielle Integrität
- Integrität physischer Güter
- Kritische Infrastrukturen.

Ein effektiver Schutz dieser Werte hängt wesentlich von der Bereitstellung und der Kontrolle der digitalen Infrastruktur ab und basiert auf mehreren Säulen:

1. Hohes Maß an Versorgungssicherheit
2. Transparenz bezüglich aller Systeme und deren Eigenschaften
3. Starker Schutz gegen unerwünschte Manipulation der Systeme.

Abbildung 1: IT-Abhängigkeiten im internationalen Kontext zeigt in vereinfachter Form die wesentlichen Elemente einer digitalen Infrastruktur und deren Herkunft.

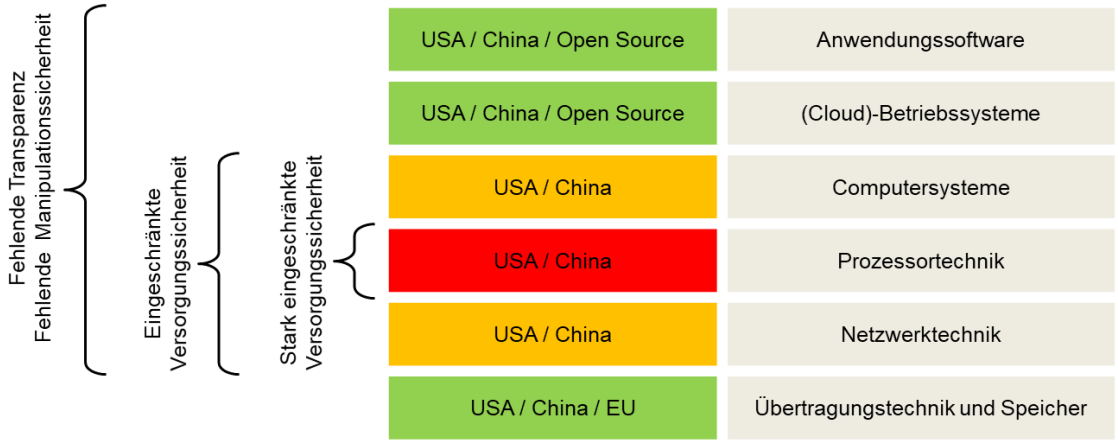

Abbildung 1: IT-Abhängigkeiten im internationalen Kontext

Daraus wird deutlich, dass aktuelle Abhängigkeiten der Digitalen Souveränität entgegenstehen:

- Eine vollständige Abhängigkeit von außereuropäischen Lieferanten besteht bei Netzwerktechnik, Prozessortechnik und Computersystemen.
- In der Übertragungstechnik gibt es wettbewerbsfähige europäische Angebote.
- Bei Betriebssystemen und Anwendungssoftware bietet Open Source realistische Alternativen zu den dominanten Anbietern.

Aus der bestehenden Situation resultieren starke Abhängigkeiten, die eine digitale Souveränität heute verhindern:

a) Stark eingeschränkte Versorgungssicherheit bezüglich IT-Komponenten bei
   - Computersystemen und deren Bausteinen (Server und Clients aller Art)
   - Prozessoren, Speicher und weitere Komponenten für die industriellen IT-Systeme
   - Netzwerktechnik für alle Arten von Computernetzen (Office IT, industrielle Systeme)

b) Fehlende Transparenz bezüglich der Steuersysteme und Betriebssoftware

c) Fehlende Manipulationssicherheit führt zu
   - gefährdeter Vertraulichkeit der Daten und Anwendungen (eingebaute "Back Doors" und eventuelle Überwachungsfunktionen)
   - gefährdeter Verfügbarkeit der Systeme und Kontrollverlust, Gefahr durch eventuell bestehende Abschaltmöglichkeiten ("Kill Switch")

- Verlust der Integrität der Daten und Anwendungen.

Diese Abhängigkeiten führen im Rahmen der fortschreitenden Digitalisierung und Vernetzung von Wirtschaft, Verwaltung und Gesellschaft zu signifikanten Risiken hinsichtlich des Schutzes der wesentlichen Werte der Digitalen Souveränität und somit zu wachsenden Risiken bezüglich der Gewährleistung der unabhängigen Funktion des öffentlichen Lebens und der Wirtschaft. Die Situation ist für Deutschland und die EU untragbar und bedrohlich für die zukünftige Entwicklung. Gesamtgesellschaftlich sollten deshalb folgende Ziele verfolgt werden:

1. Signifikant höheres Niveau bezüglich Vertraulichkeit, Integrität und Verfügbarkeit für Plattform- und Cloud-basierte Informationstechnik,
2. IT-Sicherheit wird auf ein adäquates Niveau für Geheimnisschutz, Datenschutz, Anonymisierung & Schutz von (kritischer) Infrastruktur gehoben,
3. Gewährleistung der Versorgungssicherheit.

Da die Abhängigkeit Deutschlands und der EU von außereuropäischen Lieferanten über Jahrzehnte gewachsen ist, sind Lösungen erforderlich, die mit tragbarem Aufwand innerhalb eines Zeitraums von wenigen Jahren zu einer signifikanten Verbesserung führen. Folgende Umsetzungsoptionen, siehe auch

Abbildung 2: Umsetzungsoptionen zur Reduzierung der Abhängigkeit, werden als realistisch erachtet:

1. Förderung des Einsatzes von Open Source Software in allen Bereichen von Wirtschaft und Gesellschaft,
2. Auswahl und Förderung alternativer Angebote in den Bereichen Netzwerktechnik und Computersystemen inklusive der Schlüsselkomponenten aus europäischen Quellen, bei denen die Bereitstellung aus den Quellen USA und China als nicht ausreichend bewertet wird,
3. Förderung von Entwicklung und Anwendung von Konzepten und Lösungen zur Realisierung von Transparenz und Manipulationssicherheit bestehender Systeme mittels automatischer Systeme für separate Kontrolle (Auditierung) und Steuerung (Confidential und Zero Trust Computing).

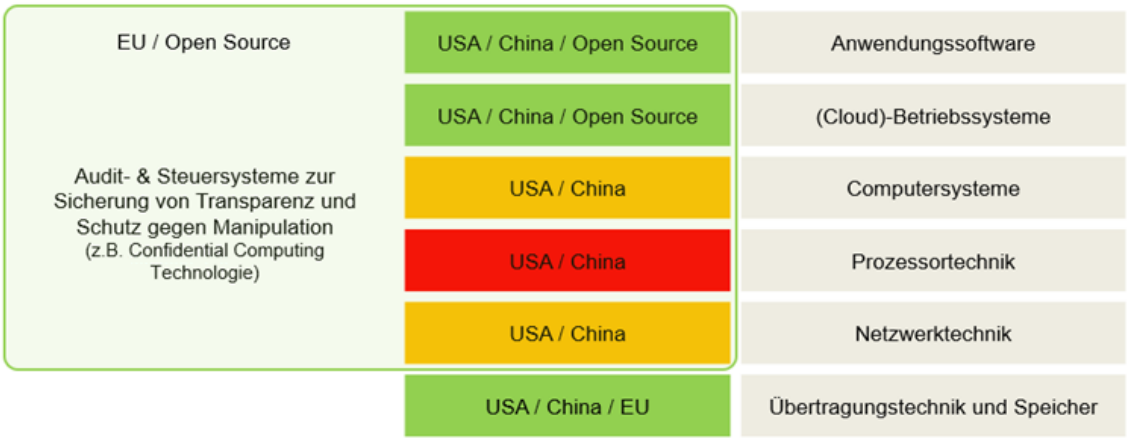

Abbildung 2: Umsetzungsoptionen zur Reduzierung der Abhängigkeit

Eine Position in diesem Sinne wurde vom Zentralverband Elektrotechnik- und Elektronikindustrie e. V. (ZVEI) in enger Zusammenarbeit mit TeleTrusT bereits 2015 erarbeitet.[3] Eine entsprechende Adjustierung der Ausrichtung ist in Deutschland bis heute nicht feststellbar.

4 Exkurs: Herausforderung Vertrauenswürdigkeit von Systemen

Der renommierte Sicherheitsforscher Bruce Schneier formuliert die paradoxe Situation treffend:

"Generell steigen Bedrohungen für Systeme mit der wachsenden Komplexität der Systeme. Es ist schon kaum möglich, ein vertrauenswürdiges System aus ausschließlich vertrauenswürdigen Komponenten aufzubauen. Da solche Komponenten in der Praxis zudem kaum verfügbar sind, stehen wir vor der Herausforderung, vertrauenswürdige Systeme aus NICHT-vertrauenswürdigen Komponenten aufzubauen. Das ist eine Aufgabenstellung, für die es aktuell keine Lösung gibt."[4]

Allerdings gibt es keine Alternative zum Finden einer Lösung. Diese Aufgabe muss als wesentliches Ziel festgelegt und angegangen werden.

Im Rahmen der Arbeit an der Erreichung dieses Ziels sollten zunächst wesentliche Lösungskomponenten identifiziert werden, die dann vorrangig von in EU ansässigen Lieferanten entwickelt und geliefert werden. Ansätze der Produktionsüberwachung und lückenlose Überwachung und Kontrolle der Lieferkette sind so konzipier- und realisierbar. Ein weiterer wesentlicher Aspekt vertrauenswürdiger Systeme ist der Nachweis der Vertrauenswürdigkeit mittels Zertifikaten. Der heutige Prozess der Zertifizierung ist jedoch der dynamischen Entwicklung der Technologie und Systeme nicht angemessen. Systeme unterliegen einer ständigen Weiterentwicklung und Verbesserung. Zertifizierungen im Abstand von einem oder mehreren Jahren liefern nur eine Momentaufnahme, die schon nach Tagen nicht mehr gültig sein muss. Hier wäre eine kontinuierliche Überprüfung der jeweiligen Systeme im Sinne einer dynamischen Attestierung sinnvoll. Dafür wären entsprechende Zertifikate, Prüfverfahren und Technologien zu entwickeln, die einen kontinuierlichen Nachweis der Einhaltung aller Maßnahmen zur vertrauenswürdigen Arbeit eines Systems bieten.

Das Ziel der Auflösung des Widerspruchs, aus nicht vertrauenswürdigen Komponenten vertrauenswürdige Systeme aufbauen zu wollen, besteht weltweit, so dass sich sehr attraktive Marktchancen für Lösungen europäischer Anbieter bei Produkten und Prozessen eröffnen.

5 Praxis-Pilot: Souveräner GAIA-X-Knoten

Unter der Bezeichnung GAIA-X hat das Bundesministerium für Wirtschaft und Energie (BMWi) eine Initiative zur Erreichung Digitaler Souveränität bei Datenplattformen und Cloud-Systemen beschrieben. GAIA-X soll den Anwendern die volle Kontrolle über ihre Daten gewährleisten, indem sie Knoten beauftragen, die gestellte Erwartungen hinsichtlich Digitaler Souveränität erfüllen.

Prinzipiell können sich alle Arten von Cloud-Anbietern am GAIA-X-System beteiligen, d.h. aus der EU sowie von außerhalb der EU. Für Anwendungsbereiche mit besonders hohen Sicherheitsanforderungen wie Gesundheitswesen, KRITIS, öffentliche Auftraggeber, Sicherheitsbehörden und weitere sind GAIA-X-Knoten mit garantierter Vertrauenswürdigkeit von besonderer Bedeutung. Für diese Anwendergruppen sind die vorliegenden Betrachtungen zu "Secure Platform" von besonderer Wichtigkeit. Auch deren Anwendungen und Prozesse entwickeln sich stärker in die Richtung von Cloud-Systemen, die dann aber adäquat bezüglich Vertrauenswürdigkeit, Zuverlässigkeit, Datenschutz und IT-Sicherheit sein müssen.

Die Realisierung eines souveränen GAIA-X-Knotens repräsentiert eine exzellente Möglichkeit zur praktischen Umsetzung einer "Secure Platform", da auf diese Weise genau die kritischen Einsatzgebiete adressiert werden und GAIA-X auch für kritische Infrastrukturen und Anwendungen genutzt werden könnte.

Der souveräne GAIA-X-Knoten wäre die Pilotrealisierung eines definierten, vertrauenswürdigen Systems, bestehend aus nicht vertrauenswürdigen Komponenten. Im Rahmen der Realisierung würden u.a.

- vorrangig EU-Komponenten eingesetzt werden,
- ein Steuersystem realisiert werden, das die Kontrolle über nicht vertrauenswürdige Komponenten ermöglicht,
- Bedarf für zwingend erforderliche EU-Komponenten identifiziert werden.

Dieser Pilot sollte von Anfang an von interessierten TeleTrusT-Mitgliedern im Rahmen der GAIA-X-Initiative eingebracht und mitgestaltet werden.

6 Umsetzung Digitaler Souveränität: Handlungsempfehlungen

6.1 Unterstützung durch Politik und staatliche Organe

Um Hersteller und Betreiber von IT-Schlüsselkomponenten - wie KRITIS-Kernkomponenten, GAIA-X-Knoten, 5G-Router oder jede andere Form von Technologie mit besonderen Sicherheitsanforderungen - dabei zu unterstützen, die beschriebenen Zielsetzungen hinsichtlich IT-Sicherheit der Systeme und Dienste zu erreichen, kommt der Politik und den staatlichen Einrichtungen aufgrund der im Vergleich zu anderen Sektoren eng gesetzten gesetzlichen und regulatorischen Rahmenbedingungen eine besondere Verantwortung zu. Ihnen stehen hierzu auch besondere Mittel zur Verfügung.

6.1.1 Regelungsrahmen, Vorbildfunktion und staatliche Beschaffung

Bei Beschaffungsverfahren des Staates für seine eigene Infrastruktur sollten die staatlichen Stellen eine Vorbildfunktion wahrnehmen, indem sie bei Ausschreibungen für Schlüsselkomponenten regelmäßig hohe Anforderungen an die IT-Sicherheit dieser Komponenten und zugehöriger Dienste stellen. Dies geschieht am geeignetsten durch Einfordern entsprechend offener, EU-weiter Standards für die IT-Sicherheit zertifizierter Produkte.

Durch den ausschließlichen Einsatz zertifizierter Produkte ergeben sich mehrere Vorteile. Zum einen wird der staatliche Beschaffungsprozess vereinfacht, da auf einen Katalog von Zertifizierungen zurückgegriffen werden kann. Hierdurch werden sowohl Ersteller von Ausschreibungen und einfachen Beschaffungen wesentlich entlastet als auch die Prüfung eingehender Angebote stark vereinfacht. Zum anderen entsteht durch gezielte Beschaffung zertifizierter Produkte durch den Staat eine indirekte, niederschwellige Förderung der Hersteller hinsichtlich IT-Sicherheit gehärteter Produkte. Um die Ziele der Digitalen Souveränität dabei bestmöglich zu unterstützen, sollten solche Produkte regelmäßig von Herstellern aus Deutschland und EU-Ländern stammen.

Schließlich wird dieses Vorgehen auch eine weitergehende Ausstrahlung über die eigene, staatliche Beschaffung hinaus entfalten. Einerseits nimmt der Staat dadurch eine Vorbildfunktion ein, indem er bei der von ihm selbst betriebenen Infrastruktur und deren Schlüsselkomponenten regelmäßig auf adäquate IT-Sicherheit der eingesetzten Produkte achtet und hierfür standardisierte Zertifizierungen einfordert. Andererseits profitieren von dieser indirekten Förderung auch privatwirtschaftliche Betreiber und Anbieter aller Unternehmensgrößen, da IT-Produkte durch Zertifizierungen einfacher vergleichbar werden, sich Beschaffungsprozesse ebenfalls vereinfachen lassen und entsprechende Produkte auch im Markt verfügbar sind.

Beispiel:

Im ICCF-Projekt[5] der Thematic Group IACS Cybersecurity Certification Framework (ICCF) des European Reference Network for Critical Infrastructure Protection (ERNCIP)[6] haben nationale Agenturen für IT-Sicherheit, Hersteller, Systemintegratoren, Anwender, Prüflabore, und das Joint Research Centre der EU[7] zunächst ein Zertifizierungsschema mit vier Zertifizierungsniveaus definiert, um anschließend in einer Machbarkeitsstudie ein existierendes Produkt anhand dieses Schemas zu zertifizieren. Der Ergebnisbericht dieses Experiments[8] stellt als primäre, weiterführende Aufgabe die mindestens EU-weite, technische Standardisierung von Schutzklassen ("Protection Profiles") und Bauartmustern ("Security Targets") fest.

Zusammenfassend wäre es daher wünschenswert,

- in der staatlichen Beschaffung von Infrastruktur-Schlüsselkomponenten einerseits Mindestanforderungen an die Zertifizierung der IT-Sicherheit entsprechend den Empfehlungen des ICCF Projekts in den Verfahrensvorschriften zur Beschaffung festzulegen, und andererseits durch eine entsprechende Ausstattung mit Finanzmitteln die Beschaffung zertifizierter Produkte zu ermöglichen,
- bei staatlichen Ausschreibungen für Infrastruktur-Schlüsselkomponenten Bewertungspunkte für "IT security made in Germany"[9] bzw. "IT security made in EU" zu vergeben,
- in den gesetzlichen und/oder regulatorischen Rahmenbedingungen für privatwirtschaftliche Betreiber Mindestzertifizierungsniveaus für die IT-Sicherheit von eingesetzten Schlüsselkomponenten entsprechend den Empfehlungen des ICCF-Projekts festzulegen und bei Unterschreitung dieser Mindestanforderungen dem Risikopotential angemessene Haftung und Sanktionen festzusetzen.

6.1.2 Förderprogramme IT-Sicherheit

Die deutschen Unternehmen mit dem Schwerpunkt IT-Sicherheit sind fast ausschließlich mittlere, kleine und Kleinstunternehmen. Diese haben bei Ausschreibungen zur öffentlichen Beschaffung und zur Forschungsförderung jedoch in der Praxis kaum Zugang, da hierbei regelmäßig Mindestanforderungen an Alter, Umsatzvolumen, und Unternehmensgröße gestellt werden, die deutsche Anbieter von IT-Sicherheit i.d.R. von solchen Ausschreibungen ausschließen.

Zu "made in Germany" gehört andererseits aber auch, dass alle deutschen Unternehmen ein angemessenes Augenmerk auf die eigene IT-Sicherheit legen. Start-ups und anderen Neugründungen fehlen jedoch meist die Finanzmittel, um entsprechende Beratungsleistungen in Anspruch nehmen zu können.

Zusammenfassend wäre es daher wünschenswert,

- das Vergaberecht dahingehend weiter zu entwickeln, dass sich bei Produkten und Dienstleistungen mit Bezug zur IT-Sicherheit lokale und junge Anbieter an solchen Ausschreibungen beteiligen können,
- dass im Bereich IT-Sicherheit, zusätzlich zur bereits vorhandenen Messeunterstützung, auch Fördermittel in bestehende Unternehmen (Entwicklungsförderung) und passende Start-ups (Gründungsförderung) investiert werden,
- dass Unternehmen ohne Fokus auf IT-Sicherheit, die Gründungsförderung erhalten, einen festgelegten Anteil dieser Fördermittel für Beratungsleistungen zur Stärkung der eigenen IT-Sicherheit verwenden müssen.

6.1.3 Eigeninitiative des Bundes

Unter den KRITIS-Unternehmen kommen der Informationstechnik und Telekommunikation besondere Bedeutung zu, da diese für Steuerung und Betrieb anderer KRITIS-Unternehmen intensiv genutzt werden. Zwar hält jeder Betreiber von KRITIS eigene Informations- und Kommunikationswege vor, jedoch erlauben ihm diese nur eine Kommunikation zwischen eigenen Einrichtungen. Verbindungen mit Einrichtungen anderer Betreiber sind so nicht möglich. Hierdurch wird ein Schwarzstart, d.h. eine Wiederinbetriebnahme nach einem großflächigen Ausfall, wesentlich erschwert, oder sogar unmöglich. Hier besteht eine Zuständigkeitslücke sowie dringender Handlungsbedarf zur Schaffung eines vom Internet unabhängigen Kommunikationssystems, um die Schwarzstartfähigkeit aller KRITIS-Unternehmen sicherzustellen. Dies könnte z.B. durch eine Anbindung von Schlüsseleinrichtungen von KRITIS an die Netze des Bundes (NdB)[10] erreicht werden. Ein solche Anbindung sollte vorgehalten, jedoch nur im Bedarfsfall freigeschaltet werden.

Zusammenfassend wäre es daher wünschenswert,

- dass der Bund zur Unterstützung bei Schwarzstart die Anschaltung von KRITIS-Betreibern an die Netze des Bundes (NdB) bei deren Planung in geeigneter Weise vorsieht und seine Netze entsprechend ertüchtigt,
- dass der Bund in Zusammenarbeit mit den KRITIS-Betreibern eine Schnittstellen- und Protokollspezifikation für diese Anschaltung erarbeitet und deren Implementierung für alle KRITIS-Betreiber verbindlich vorschreibt,
- dass zur Unterstützung bei Schwarzstart staatenübergreifend vernetzter KRITIS-Unternehmen der Bund geeignete Verbindungen zu entsprechenden Kommunikationssystemen benachbarter EU-Staaten schafft und diese betreibt.

6.1.4 Zulassung und Zertifizierung

Die Empfehlungen des ICCF-Projekts sehen für die höchste Zertifizierungsstufe eine Zertifizierung durch staatliche Stellen vor, sowie für niedrigere Zertifizierungsstufen die Akkreditierung privatwirtschaftlicher Zertifizierungsstellen. TeleTrusT unterstützt diese Empfehlungen, da nur so ein ausreichendes Vertrauen in solche Zertifizierungen gewährleistet werden kann.

Ein neues Produkt nach 27 unterschiedlichen Schemata zertifizieren zu lassen, würde ein unverhältnismäßiges Investitionshemmnis im ohnehin durch Kleinstmengen geprägten KRITIS-Markt darstellen. Zudem würde hierdurch der Marktzugang für neue Anbieter praktisch unmöglich. Damit sich Akkreditierung und Produktzertifizierungen nicht als Investitionshemmnis, sondern investitionsfördernd auswirken, sollten daher EU-weite Zertifikate eingeführt werden. Neben der oben beschriebenen Vereinfachung der Ausschreibungs- und Beschaffungsprozesse entsteht durch eine EU-weit einheitliche Regelung ein größerer Markt, was aus TeleTrusT-Sicht entscheidend für eine erfolgreiche Durchsetzung solcher Zertifizierungen sein wird.

Zusammenfassend wäre es daher wünschenswert,

- dass sich die Bundesregierung im Europäischen Rat sowie der Europäischen Kommission aktiv für die Schaffung eines EU-weiten, transparenten Zertifikate-Schemas entsprechend den Empfehlungen des ICCF-Projekts einsetzt,

- dass sich die Bundesregierung im Europäischen Rat sowie der Europäischen Kommission aktiv dafür einsetzt, dass bei der Beschaffung von IT-Schlüsselkomponenten durch staatliche wie privatwirtschaftlichen Stellen ein dem Risikopotential angemessenes Mindestzertifizierungsniveau verbindlich vorgeschrieben wird,
- dass hierbei für KRITIS-Kernkomponenten regelmäßig hohe und höchste Anforderungen zu stellen sind,
- dass die staatlichen Anforderungen für Zertifizierung und Akkreditierung umfassend dokumentiert werden und diese Informationen im Internet kostenlos und frei zugänglich sind,
- dass zusätzlich zu den Anforderungen, kostenlose, unterstützende Informationen - wie z.B. Prüflisten - im Internet bereitgestellt werden, um Antragsteller bei ihrer Vorbereitung bestmöglich zu unterstützen,
- dass jede Akkreditierungs- und Zertifizierungsstelle dazu verpflichtet ist, eine jederzeit aktuelle Liste ausgegebener, erloschener und widerrufener Akkreditierungen bzw. Zertifizierungen frei zugänglich im Internet zu veröffentlichen.

6.1.5 Begleitung und Förderung des Standardisierungsprozesses

Die Vorarbeiten des ICCF-Projektes (siehe auch dessen Ergebnisbericht 2017) waren auf die Definition eines prozeduralen Gerüstes sowie auf die Bestimmung geeigneter Zertifizierungsstufen gerichtet. Als noch zu bearbeitendes Gebiet wurden technische Standards und Architekturmuster identifiziert, die diese Schutzstufen technisch definieren bzw. umsetzen helfen. In dieser technischen Arbeit werden sich TeleTrusT-Mitglieder engagieren (siehe 6.3).

Um hierbei zu gewährleisten, dass die in die technische Standardisierung einfließenden Maßstäbe und Mechanismen zur IT-Sicherheit von Schlüsselkomponenten nicht im Widerspruch zu solchen für andere, staatlich beschaffte IT-Produkte stehen oder hinter diesen zurückbleiben, sollte die Arbeit der TeleTrusT-Mitglieder im technischen Standardisierungsprozess durch relevante, nationale Organe der IT-Sicherheit unterstützt und begleitet werden.

In der Praxis sind deutsche Akteure jedoch in der einschlägigen Normung und Standardisierung wenig aktiv. Akteure aus anderen Ländern setzen hier die Maßstäbe und deutsche Hersteller implementieren im Nachgang lediglich die Ergebnisse, ohne vom Technologie- und Erfahrungsaustausch in den Standardisierungsgremien oder dem Zeitvorteil durch frühe Kenntnis des zukünftigen Standards profitieren zu können. Oft können gerade innovative, kleine Unternehmen aus finanziellen Gründen nicht an der Normung und Standardisierung teilnehmen und so ihre innovativen Ideen und Produkte nicht durchsetzen.

Zusammenfassend wäre es daher wünschenswert,

- dass kleine, innovative Unternehmen aus dem Bereich IT-Sicherheit durch geeignete Förderung in die Lage versetzt werden, sich aktiv an Normungs- und Standardisierungsprozessen zu beteiligen,
- dass sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) und die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (ZITiS) an der technischen Normung und Standardisierung im European Telecommunications Standards Institute (ETSI) zur technischen Umsetzung eines Zertifizierungsrahmens entsprechend den Empfehlungen des ICCF-Projekts an der Seite der TeleTrusT-Mitglieder aktiv beteiligen, insbesondere durch Entsendung jeweils eines/einer Delegierten,
- dass die Bundesregierung aktiv darauf hinwirkt, dass die erarbeiteten Standards, Zertifizierungen und Akkreditierungen zu Schlüsselkomponenten für eben diesen Bereich von der European Union Agency for Cybersecurity (ENISA) als Bestandteil ihres EU Cybersecurity Certification Framework[11] übernommen werden.

6.2 Unterstützung durch Anwender in Industrie und im Dienstleistungssektor

Um die Sicherheit eines Systems und der von diesem erbrachten Dienste gewährleisten zu können, müssen vier Bereiche betrachtet werden:

- verwendete Normen und Standards,
- Implementierung,
- Konfiguration,
- Betrieb.

Bleiben einer oder mehrere dieser Bereiche unberücksichtigt, ist die Sicherheit des Systems nicht mehr gegeben. Hersteller und Anwender tragen also eine substantielle Eigenverantwortung, diese Bereiche jederzeit abzudecken. Besonderes Augenmerk muss dabei auf die Systemintegration gelegt werden, da diese einen Überschneidungsbereich zwischen Hersteller und Anwender darstellt und daher von beiden in enger Kooperation bearbeitet werden muss.

6.2.1 Eigene Bewertungskompetenz stärken

Wenn niemand etwas weiß, ist jeder ein Experte.

Wenn Jeder ein Experte wäre, würde es keinen Sinn ergeben, Experte werden oder als solcher gelten zu wollen.

Im Spannungsfeld dieser beiden Aphorismen bewegen sich manche Unternehmen, wenn es um die IT-Sicherheit der von ihnen aufzubauenden Anlagen und Systeme geht. Einerseits bewerben die Lieferanten und Hersteller der einzelnen Komponenten regelmäßig die hervorragende Sicherheit ihrer Produkte und beschreiben die vorhandenen Absicherungen. Andererseits können Komponentenhersteller und -lieferanten jedoch keine Aussage darüber treffen, wie der Schutzbedarf des Kunden aussieht, ob die IT-Sicherheitsmechanismen ihrer Produkte diesen Schutzbedarf abdecken und wie die Schutzmechanismen sich bezüglich der konkreten Bedrohungslage des Kunden einordnen. Umso weniger können solche Aussagen von einem Lieferanten oder Hersteller getätigt werden, wenn der Kunde selbst die Integration der Produkte in sein Gesamtsystem vornimmt.

Zusammenfassend wäre es daher wünschenswert,

- von neutralen und produktunabhängigen Beratungs- und Schulungsangeboten zur IT-Sicherheit Gebrauch zu machen, um eine angemessene, eigene Bewertungskompetenz für sichere Lösungen auf- bzw. auszubauen,
- zu einer realistischen Einschätzung der eigenen IT-Sicherheits-Kompetenz zu gelangen, d.h. sich selbst in die Lage versetzen zu erkennen, wenn eine Entscheidung die eigene Kompetenz überfordert,
- die eigene Strategie dahingehend zu erweitern, dass in einem solchen Fall regelmäßig von neutralen und produktunabhängigen Beratungsangeboten zur IT-Sicherheit Gebrauch gemacht wird und hierbei auf "IT security made in Germany" bzw. "made in EU" zu achten.

6.2.2 Eigene Compliance stärken und Haftungsrisiken reduzieren

In *6.1* wird angeregt, durch dem Risiko angemessene Haftungsregelungen und Sanktionen gesetzliche bzw. regulatorische Anreize zur geeigneten Festlegung und Umsetzung einer IT-Sicherheitsstrategie der Betreiber und Hersteller zu setzen. Selbst wenn der Gesetzgeber hierbei letztlich Milde walten lassen sollte, bleiben stets zivil- und handelsrechtliche Schadensersatzansprüche, die bei durch Verwundbarkeit der eigenen IT verursachten Ausfällen entstehen können. Betreiber und Hersteller müssen daher stets bestrebt sein, Ausstattung und Betrieb am Stand der Technik[12] zu orientieren und schon bei der Beschaffung die IT-Sicherheit von Komponenten mindestens gleichwertig mit dem Preis zu bewerten.

Zusammenfassend wäre es daher wünschenswert,

- bei anderweitig nahezu gleichwertigen Alternativkomponenten regelmäßig anstatt der billigeren, diejenigen mit dem höheren IT-Sicherheitsniveau vorzuziehen,
- die Ausrichtung am Stand der Technik und die Durchführung einer IT-Sicherheitsbewertung systematisch als festen Bestandteil aller Entwurfs-, Konstruktions-, und Beschaffungsvorgänge in der eigenen Compliance zu verankern, um dadurch letztlich Sanktions-, Haftungs-, und Schadensersatzrisiken zu minimieren.

6.2.3 Eigene Kompetenz zur Systemintegration auf- bzw. ausbauen und auf EU-weit standardisierte Zertifizierungen setzen

Für komplexe industrielle Systeme und Anlagen existieren keine fertigen Komplettlösungen. Hierfür unterscheiden sich die jeweiligen Anforderungen und Anwendungsfälle zu stark. Daher muss der Betreiber eines solchen Systems die Einzelkomponenten entweder selbst zu einem Gesamtsystem integrieren oder dies von einem Systemintegrator als Dienstleistung bewerkstelligen lassen. Zur Vermeidung von Abhängigkeiten und um auch bei einem Ausfall des Dienstleisters handlungsfähig zu bleiben, werden Betreiber i.d.R. eigene Experten und Konstrukteure an der Systemintegration beteiligen, um so internes Know-how über die eigenen Systeme aufzubauen und zu erhalten.

Dabei wird das Hauptaugenmerk regelmäßig auf die unmittelbar den Primärfunktionen der Anlage dienenden Aspekte gelegt und die Sicherheit der eingesetzten IT-Komponenten erst im Nachgang oder gar nicht betrachtet. Ein solches Vorgehen wird regelmäßig zum Auftreten von Verwundbarkeiten der IT-Komponenten und des Gesamtsystems führen. Der einzige erfolgversprechende Weg, um diese Verwundbarkeiten zu vermeiden, ist es, die Anforderungen an die IT-Sicherheit der Komponenten sowie des Gesamtsystems im Entwurfsprozess von Anfang an

gleichberechtigt neben den übrigen Anforderungen zu betrachten. Dies allein ist jedoch nicht ausreichend, da auch Entwurfs- und Implementierungsfehler in den selbst erstellten Integrationskomponenten Verwundbarkeiten hervorbringen können. Um dieses Risiko zu minimieren, muss auch der Entwicklungsprozess selbst Sicherheitsanforderungen genügen.

Zusammenfassend wäre es daher wünschenswert,

- dass europäische Standards genutzt werden, um die eigenen Prozesse zur Systemintegration als Secure-by-Design zu zertifizieren (existierende europäischen Standards in diesem Bereich wie z.B. IEC 62443 decken den Bedarf insbesondere im Bereich KRITIS nicht vollständig ab. TeleTrusT-Mitglieder werden sich daher in die europäische Normung aktiv einbringen, um diese Lücken zu schließen; *siehe 6.3*),
- entsprechende Sicherheitszertifizierungen für Prozesse und Produkte regelmäßig von Lieferanten und Dienstleistern einzufordern.

6.3 Unterstützung durch Hersteller von IT- und IT-Sicherheitsprodukten

Um Hersteller und Anwender von Schlüsselkomponenten in ihren Bemühungen dabei zu unterstützen, ihre jeweiligen Systeme sicher zu gestalten und zu betreiben (vgl. *6.2*), werden interessierte TeleTrusT-Mitglieder ihre Kompetenzen bündeln und sich insbesondere in den Bereichen Normung und Standardisierung sowie bei Informations- und Aufklärungsangeboten, in denen einzelne Hersteller und Anwender mitunter nur schwer aktiv werden können, engagieren.

6.3.1 Engagement in der technischen Standardisierung zur Umsetzung eines EU-weiten Zertifizierungssystems

Wichtige Vorbereitungen zur Einführung eines EU-weiten Zertifizierungsschemas wurden bereits im ICCF-Projekt geleistet. Der Titel des Projekts suggeriert zwar zunächst eine Beschränkung auf industrielle Automatisierungssysteme (Industrial Automation and Control Systems, Abkürzung IACS), im Projekt wurden jedoch gesamtheitlich industrielle Firewalls, Datendioden und ähnliche, der industriellen IT zuzuordnende Produkte betrachtet. Moderne Industrieautomatisierung ist immer auch IT und wird auch in KRITIS eingesetzt.

Im genannten EU-Projekt haben nationale Agenturen für IT-Sicherheit, Hersteller, Systemintegratoren, Anwender, Prüflabore und das Joint Research Centre der EU zunächst ein Zertifizierungsschema mit vier Zertifizierungsniveaus definiert, um anschließend in einer Machbarkeitsstudie ein existierendes Produkt anhand dieses Schemas zu zertifizieren. Der Ergebnisbericht dieses Experiments stellt in seinem Ergebnis als primäre, weiterführende Aufgabe die mindestens EU-weite, technische Normung und Standardisierung von Schutzklassen ("Protection Profiles") und Bauartmustern ("Security Targets") fest.

In genau diesem Bereich der technischen Normung und Standardisierung auf europäischer Ebene werden sich interessierte Mitglieder des TeleTrusT engagieren. Sie werden die Zusammenarbeit mit dem ICCF-Projekt, ETSI und europäischen Partnern aus der Wirtschaft suchen, um entsprechende, geeignete EU-Standards für Schutzklassen ("Protection Profiles") und Bauartmuster ("Security Targets") zu erarbeiten und als europäische Normen zu veröffentlichen, um hierdurch die praktische Umsetzung des vom ICCF-Projekt vorgeschlagenen Zertifizierungssystems zu ermöglichen.

TeleTrusT und seine Mitglieder haben sich in diesem Umfeld bereits engagiert und Ansehen erarbeitet. So wird die in der Praxis sehr erfolgreiche internationale Normenreihe IEC 62443 über "Industrielle Kommunikationsnetze - IT-Sicherheit für Netze und Systeme" umgangssprachlich oft als "TeleTrusT Specification" bezeichnet, da sie in wesentlichen Teilen durch die Mitarbeit von TeleTrusT-Mitgliedern ermöglicht wurde. Zudem hat die ENISA die TeleTrusT-Handreichung zum "Stand der Technik in der IT-Sicherheit" ins Englische übersetzen lassen. Diese Übersetzung wurde von TeleTrusT und ENISA im Namen beider Organisationen veröffentlicht.[13]

Für den Erfolg des Engagements von TeleTrusT bzw. seiner Mitglieder in der europäischen Normung sind Unterstützung und Begleitung durch die deutsche Politik (vgl. *6.1*) ein entscheidender Faktor, ebenso wie für die Implementierung eines europäischen IT-Sicherheitszertifikats für IT-Schlüsselkomponenten.

6.3.2 Bereitstellen sicherer Produkte

Durch ihre aktive Beteiligung an der technischen Normung und Standardisierung werden die involvierten TeleTrusT-Mitglieder frühzeitig Kenntnis von künftigen, technischen Normen erlangen. Diese können und werden sie in ihre Produktentwicklung einfließen lassen, um als frühzeitig mit geeigneten, zertifizierten Produkten am Markt präsent zu sein. Diese Produkte werden auf einer sicheren Hardware- und Softwareplattform basieren, die die in der technischen Standardisierung erarbeiteten Bauartmuster ("Security Targets") umsetzt und gleichzeitig deren Skalierung zur Erreichung der verschiedenen Schutzklassen ("Protection Profiles") gestattet. Die Absicht, eine solche sichere Plattform bereitzustellen, hat interessierte TeleTrusT-Mitglieder im Arbeitskreis "Secure Platform" zusammengeführt. Da die Definition und Entwicklung einer solchen "Secure Platform" komplex ist, kann dies innerhalb von TeleTrusT nur durch Bündelung der Ressourcen mehrerer Unternehmen erreicht werden. Einige Mitglieder des TeleTrusT-Arbeitskreises "Secure Platform" haben sich daher darauf verständigt, sowohl die Mitarbeit an der technischen Standardisierung als auch mindestens die Machbarkeitsstudien zur Vorbereitung der Produktentwicklung in einer vorwettbewerblichen Zusammenarbeit gemeinsam zu leisten. Ein solches, hieraus entstehendes Produkt könnten zum Beispiel GAIA-X Knoten hoher und höchster Sicherheitsstufen sein.

Die Verfügbarkeit von geeigneten Produkten allein sichert jedoch noch nicht deren Einsatz. Um dies zu erreichen, muss es den Anwendern dieser Produkte ermöglicht werden, solche Angebote aufzufinden und zu bewerten. Am einfachsten wird dies durch einen zentralen Katalog erreicht, der verzeichnet, für welche Einsatzzwecke und Problemstellungen Produkte von EU-Herstellern verfügbar sind. TeleTrusT wird sich in seiner europäischen Zusammenarbeit für die Schaffung eines solchen Kataloges einsetzen und sich an dessen Umsetzung beteiligen. Um eine Bewertung durch Anwender zu ermöglichen, muss dieser Katalog neben der Auflistung verfügbarer Produkte auch auf öffentlich verfügbare Informationen über vorhandene Schwachstellen in Produkten enthalten.

6.3.3 Informations- und Aufklärungsangebote schaffen und ausbauen

Aus dem Gesamtbild der im vorliegenden Positionspapier vorgestellten Handlungsempfehlungen lässt sich unter anderem ablesen, dass viele grundlegende Fehler in Bezug auf IT-Sicherheit aus Mangel an Informationen und mangelndem Problembewusstsein resultieren. Um dem begegnen zu können, sind zwei Dinge erforderlich: Zum einen muss der Mangel erkennbar gemacht werden und zum anderen müssen geeignete Informationen auffindbar und verständlich sein, um Lücken schließen zu können.

TeleTrusT kann und wird daher in Zusammenarbeit mit seinen Mitgliedern die TeleTrusT-Handreichung zum "Stand der Technik in der IT-Sicherheit" stetig fortentwickeln sowie versuchen, diese Publikation so breit wie möglich bekannt zu machen und an betroffene und interessierte Organisationen heranzutragen.

Desweiteren wird TeleTrusT diejenigen Mitglieder, die zur Nutzung des Vertrauenszeichens "IT Security made in Germany" berechtigt sind, dazu ermuntern, insbesondere in der Werbung für Produkte, die für den Einsatz in KRITIS vorgesehen oder geeignet sind, dieses Siegel durchgehend und prominent einzusetzen. Die konsistente und anhaltende Nutzung dieses Zeichens, insbesondere wenn dieses in elektronischen Dokumenten mit einem Web-Link hinterlegt ist, ist ein einfacher und oft effektiver Weg, um Anwendern einen Einstieg in eigene Recherchen und eine Beschäftigung mit IT-Sicherheit nahezulegen.

7 Referenzen

[1] BMWi, (2019). Das Projekt GAIA-X. https://www.bmwi.de/Redaktion/DE/Publikationen/Digitale-Welt/das-projekt-gaia-x.pdf (17.12.2019)

[2] BSI, (2019). Die Lage der IT-Sicherheit in Deutschland 2019. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2019.pdf (17.12.2019)

[3] ZVEI, (2015). Diskussionspapier Digitale Souveränität. Debatte über einen besonnenen Umgang mit internationalen Herausforderungen und die Stärkung des Industriestandorts Deutschland. https://www.teletrust.de/fileadmin/docs/publikationen/broschueren/Digitale_Souveränität/ZVEI_Diskussionspapier_Digitale_Souveränität.pdf (17.12.2019)

[4] Schneier Bruce, (2019). Every Part of the Supply Chain Can Be Attacked. https://www.nytimes.com/2019/09/25/opinion/huawei-internet-security.html (17.12.2019)

[5] ERNCIP, (2019). IACS Cybersecurity Certification Framework. https://erncip-project.jrc.ec.europa.eu/networks/tgs/european-iacs (17.12.2019)

[6] ERNCIP, (2019). The ERNCIP Project Platform. https://erncip-project.jrc.ec.europa.eu/ (17.12.2019)

[7] EU Joint Research Centre, (2019). EU Science Hub. https://ec.europa.eu/jrc/ (17.12.2019)

[8] ERNCIP Thematic Group: European IACS Cybersecurity Certification, (2018). IACS Cybersecurity Certification Framework (ICCF): Lessons from the 2017 study of the state of the art. https://erncip-project.jrc.ec.europa.eu/sites/default/files/JRC111611_The_IACS_Cybersecurity_Certification_Framework.pdf (17.12.2019)

[9] TeleTrusT (2019). IT security made in Germany. https://www.teletrust.de/itsmig/ (17.12.2019)

[10] Bundesministerium des Innern, für Bau und Heimat, (2019). Netze des Bundes. https://www.bmi.bund.de/DE/themen/it-und-digitalpolitik/it-des-bundes/netze-des-bundes/netze-des-bundes-node.html (17.12.2019)

[11] ENISA, (2019). EU cybersecurity certification framework. https://www.enisa.europa.eu/topics/standards/certification (17.12.2019)

[12] TeleTrusT (2019). Stand der Technik. https://www.teletrust.de/publikationen/broschueren/stand-der-technik/ (17.12.2019)

[13] TeleTrusT (2019). Was ist "Stand der Technik" in der IT-Sicherheit? ENISA und Bundesverband IT-Sicherheit e.V. (TeleTrusT) veröffentlichen Handreichung in englischer Sprachfassung. https://www.teletrust.de/fileadmin/docs/presse/presse-docs/PM-190207-ENISA-TeleTrusT-Handreichung_Stand_der_Technik_DEU.pdf (17.12.2019)