Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

"*Cyber-Nation*"

Positionspapier

2025

Zusammenfassung

Danksagung

Diese Publikation wurde in der TeleTrusT-Arbeitsgruppe "Cyber-Nation" erarbeitet. TeleTrusT bedankt sich bei den nachstehenden Personen für ihre Mitwirkung sowie für die aktive Mitgestaltung dieses Positionspapieres.

Projektleitung
Dr. Kim Nguyen, Bundesdruckerei, Leiter der TeleTrusT-AG "Cyber-Nation"

Autorenliste

Bartels, RA Karsten U. - HK2
Barth, Michael - genua
Bednarek, Timo - MB connect line
Benzmüller, Ralf – G Data
Blunk, Rolf - IFIT
Dreke, Christopher - Bundesdruckerei
Gremeyer, Erik - ATM Consulting
Heinrich, Marcus - agilimo
Heyde, Steffen - secunet
Könen, Andreas
Kruse Brandao, Jacques Olaf - TÜV Informationstechnik
Müller, Daniel - secunet
Nguyen, Dr. Kim - Bundesdruckerei
Noack, Andrew - Utimaco
Pohlmann, Prof. Dr. Norbert - if(is)
Saygin, Yakup - sayTEC
Siebert, Dr. Gunnar - Aon
Spletter, Christian - metafinanz
Wetzel, Maik - ESET

Redaktion

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

In dieser Publikation werden Anglizismen verwendet, die 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
E-Mail: info@teletrust.de
https://www.teletrust.de

Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können. Dazu hält es der Bundesverband IT-Sicherheit e.V. (TeleTrusT) für dringend erforderlich, dass Deutschland im Bereich der IT-Sicherheit und in der gesamtgesellschaftlichen Herangehensweise eine Vorreiterrolle einnimmt. Dies betrifft insbesondere Kommunikation, Kooperation und Koordination auf Basis gemeinsamer Grundwerte.

In diesem Kontext hat BSI-Präsidentin Claudia Plattner die Vision einer "Cyber-Nation Deutschland“ formuliert: Diese ist geleitet von der Überzeugung, dass wir als Staat und Gesellschaft den immer größer werdenden Bedrohungen in der Cyber-Sicherheit konsequent und mutig entgegentreten müssen. Dazu sind signifikante Anstrengungen notwendig, darüber hinaus eine effiziente und effektive Zusammenarbeit aller Akteure und eine funktionierende Koordination der notwendigen Maßnahmen (Quelle: BSI-Webseite).

Konkret werden die folgenden **sechs Ziele** auf dem Weg hin zur Cyber-Nation definiert:

1. **Cyber-Sicherheit auf die Agenda heben**
2. **Cyber-Resilienz signifikant erhöhen**
3. **Technologiekompetenz gezielt nutzen**
4. **Digitalisierung konsequent voranbringen**
5. **Cyber-Sicherheit pragmatisch gestalten**
6. **Einen florierenden Cyber-Markt Deutschland aufbauen.**

TeleTrusT ist davon überzeugt, dass die Vision der Cyber-Nation Deutschland nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden kann. Derzeit existieren im Kontext der Cyber-Sicherheit zu viele Einzelinitiativen, die kaum oder nur zu geringe Wirkung zeigen. Es bedarf daher dringend einer Umsetzungsstrategie, wie sie durch die Vision der Cyber-Nation gefordert wird, die strategische Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik, Verwaltung, Wirtschaft, Hersteller- und Anwendungsunternehmen, Recht, Gesellschaft und Forschung vornimmt. Damit ist klar, dass die Aufgabe des Aufbaus der Cyber-Nation Deutschland eine ganzheitliche ist. Die Politik ist allerdings - gerade im Hinblick auf die aktuellen Entwicklungen aus den USA[1]) - aufgerufen, den Startimpuls für die Umsetzungsstrategie zu setzen und sie langfristig zu unterstützen. Gleichwohl kann die Umsetzung der Cyber-Nation nur im erfolgreichen Zusammenspiel von Wirtschaft, Wissenschaft/Forschung, Anwendern, Politik und (Sicherheits-)Behörden gelingen. Auch weitere Stakeholder wie etwa Zivilgesellschaft, Recht, Kunst/Kultur, Militär und Medien spielen natürlich eine wesentliche Rolle.

In diesem Sinne formuliert die TeleTrusT-AG "Cyber-Nation" die folgenden zentralen Forderungen an die genannten politischen Stakeholder:

Cyber-Sicherheit auf die Agenda heben heißt:

Klares Bekenntnis zu (unbeschränkter) IT-Sicherheit und zu einem ganzheitlichen Blick auf IT-Sicherheitsarchitekturen

Bund und Länder müssen sich stärker zur IT-Sicherheit bekennen, deren Umsetzung vorantreiben und entsprechende Investitionen tätigen. Sie sind gefordert, eine Vorreiterrolle einzunehmen, indem sie mehr Zentralisierung und weniger Fragmentierung in der Cyber-Sicherheit ermöglichen.

Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und praxisorientiert

Überarbeitung und Harmonisierung der IT-Sicherheitsgesetzgebung: Die IT-Sicherheitsgesetze müssen konsequent auf die Förderung der digitalen und technologischen Souveränität Deutschlands und der EU sowie die Wahrung der Grundrechte ausgerichtet werden. Sie sollten einheitlich abgestimmt sein, um Rechtssicherheit zu maximieren und Unklarheiten zwischen nationalen und europäischen Regelungen, insbesondere beim Stand der Technik, zu minimieren.

[1] Joe Bidens Executive Order on Strengthening and Promoting Innovation in the Nation’s Cybersecurity vom 16.01.2025 und die Etablierung des 500 Milliarden USD-Projekts “Stargate” zur Etablierung neuer KI Rechenzentren in den USA

Verbot der Kompromittierung von IT-Sicherheit, keine Backdoors oder geschwächte Verschlüsselung

Deutschland darf nicht durch gesetzliche Verpflichtungen oder auf anderen Wegen die Schwächung von IT und IT-Diensten veranlassen, wo Schwachstellen bewusst durch den Staat verschwiegen werden und damit die Sicherheit der Bürgerinnen und Bürger, Unternehmen und Kritischen Infrastrukturen geschwächt wird.

Aber auch eine staatlich motivierte Schwächung von Kryptografie oder den Wünschen nach Hintertüren muss endgültig eine Absage erteilt werden.

Die Kompromittierung von IT-Sicherheit, der Einsatz von verborgenen Backdoors oder geschwächter Verschlüsselung widerspricht dem staatlichen Auftrag zur Gewährleistung einer hohen Cyber-Sicherheit und zerstört das Vertrauen in die digitale Zukunft.

Cyber-Resilienz signifikant erhöhen **heißt:**

Auf- und Ausbau von IT-Sicherheitsinfrastrukturen (sowohl technisch als auch organisatorisch) für Bürger, Unternehmen und Verwaltung fordern und fördern

Zügige Umsetzung des NIS-2-Umsetzungsgesetzes: Die neue Bundesregierung muss die Bundesverwaltung, Länder, Kommunen und Bildungseinrichtungen aktiv einbeziehen, um die Maßnahmen effizient und flächendeckend umzusetzen. Das BSI sollte in diesem Kontext als zentrale Stelle mit erweiterten Kompetenzen, zusätzlichen Ressourcen und neuen Stellen ausgestattet werden.

Die Bundesregierung muss Hersteller aktiv bei der Umsetzung des CRA unterstützen und gezielt KMUs sowie Start-ups fördern, um deren Wettbewerbsfähigkeit zu sichern.

Zügige Umsetzung der europäischen digitalen Identität: Die Bundesregierung sollte die Einführung der European Digital Identity Wallet (EUDIW) im Rahmen der europaweit vorgegebenen Zeitpläne aktiv vorantreiben und deren benutzerfreundliche Umsetzung sicherstellen. Für das Home-Office sollten qualifizierte Vertrauensdienste gemäß der eIDAS-Verordnung sowie die Integration der Konzepte der EUDIW konsequent genutzt werden, um Sicherheit und Vertrauenswürdigkeit zu erhöhen. Die zügige Umsetzung der eIDAS-Verordnung, insbesondere der Regelungen zu qualifizierten Website-Zertifikaten (QWACs) gemäß Artikel 45, muss sichergestellt werden, um Verbraucherinnen und Verbraucher besser vor gefälschten Webseiten und Datenmissbrauch zu schützen.

Standardisierung eines gemeinsamen Identitätsökosystems: Die europäischen Vorgaben für ein einheitliches Identitätsökosystem müssen schnell festgelegt und umgesetzt werden, einschließlich der Zusammenführung bestehender branchenspezifischer Systeme.

Technologiekompetenz gezielt nutzen **und** ***einen florierenden Cyber-Markt Deutschland aufbauen*** **heißt:**

Mehr und integral wirkende IT-Sicherheitstechnologie "Made in Germany/made in EU" in der Praxis

Bund und Länder müssen gezielte Förderprogramme für bestehende Unternehmen und Start-ups schaffen, um IT-Sicherheitslösungen zu entwickeln, Standards zu setzen und lokale Anbieter zu stärken. Dies umfasst auch eine Reform der Vergaberegeln, damit KMUs und junge Unternehmen besseren Zugang zu öffentlichen Ausschreibungen und Forschungsförderungen erhalten.

Schaffung eines sicheren Cloud-Ökosystems: Ein strategischer Fokus auf europäische Cloud-Lösungen mit Sicherheitsankern und vertrauenswürdiger Infrastruktur ist notwendig, um Datensouveränität zu gewährleisten. Die aktuelle Cloudstrategie des BSI sollte überarbeitet werden, um ausschließlich vertrauenswürdige Anbieter zu berücksichtigen.

Stärkung der digitalen und technologischen Souveränität: Der Ausbau unabhängiger europäischer Technologieproduktionen und sicherer Plattformen, insbesondere in der Mikroelektronik und Halbleitertechnologie, muss mit klaren Anreizen und verbindlichen Beschaffungspolitiken gezielt gefördert werden. Systemrelevanz der IT-Sicherheitsbranche anerkennen: IT-Sicherheit muss als systemrelevante Branche betrachtet werden.

Die Einbindung von kritischen Versorgungs- und Produktionsunternehmen sowie gezielte staatliche Maßnahmen sind erforderlich, um auch in Krisenzeiten die Stabilität der Volkswirtschaft und des Gemeinwesens sicherzustellen.

Digitale Souveränität im Bereich IT-Sicherheit schaffen - für eine werteorientierte, sichere und vertrauenswürdige digitale Zukunft

Es ist essenziell, die technologische Souveränität zu stärken, indem Schlüsselkompetenzen entwickelt, Abhängigkeiten reduziert und regulatorische Vorgaben sowie Zertifizierungsverfahren für sicherheitskritische Technologien geschaffen werden. Um Cloud-Angebote internationaler Anbieter nutzen zu können, müssen diese verpflichtet werden, nationale Sicherheitsanker und Technologien zur Absicherung der Services einzubinden

IT-Infrastrukturen müssen ganzheitlich und resilient gestaltet werden, um sichere Kommunikation, Business Continuity sowie Flexibilität und Skalierbarkeit zu gewährleisten, wobei bestehende Flickenteppiche durch integrierte Lösungen ersetzt werden.

Sowohl für Unternehmen als auch öffentliche Stellen muss klar sein: Beauftragungen, Ausschreibungen und laufende Vertragsverhältnisse sind hinsichtlich der IT-Sicherheit zu schärfen. Es bedarf belastbarer Vereinbarungen über IT-Sicherheitsleistungen, die unter anderem dem Umstand Rechnung tragen, dass Leistungen auch künftig dem Stand der Technik entsprechen. IT-Sicherheitsvereinbarungen sind das Schutzschild digitaler Leistungen und unserer IT-Infrastrukturen.

Mit den Vertrauenssiegeln "IT Security made in Germany/made in EU“ und durch Förderung sicherer Technologien und europäischer Harmonisierung muss der Staat eine Vorreiterrolle einnehmen und die digitale Souveränität stärken.

Cyber-Sicherheit pragmatisch gestalten **heißt:**

Cyber-Sicherheit muss konsequent bereits beim Design neuer Dienste und Architekturen mitgedacht werden, gleichzeitig ist immer wieder die richtige Balance aus Sicherheit und Nutzerfreundlichkeit zu finden.

Cyber-Sicherheit muss konsequent bereits beim Design neuer Dienste und Architekturen mitgedacht werden und selbst digital werden, insbesondere was die verwendeten Methoden und Prozesse betrifft. Gleichzeitig ist immer wieder die richtige Balance aus Sicherheit, Nutzerfreundlichkeit und möglichst nahtloser Integration zu finden. Cyber-Sicherheit pragmatisch gestalten heißt die richtige Balance aus Sicherheit und Nutzerfreundlichkeit zu finden. Absolute Sicherheit kann es nicht geben, das gilt auch für Cyber-Sicherheit. Daher sind Risiken zum einen konsequent zu bestimmen und zu bewerten, aber auch verbleibende Restrisiken in der entsprechenden Verantwortung zu akzeptieren. Nur so kann verhindert werden, dass die Nutzerfreundlichkeit auch auf den "letzten Metern" nicht wieder wesentlich eingeschränkt wird. Die wechselseitige Anerkennung von Zertifizierungsergebnissen kann Aufwände wesentlich reduzieren.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Fachleute, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Personenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie der Vertrauenszeichen "IT Security made in Germany" und "IT Security made in EU". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Telefon: +49 30 4005 4306
E-Mail: holger.muehlbauer@teletrust.de
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.