Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

"Cyber-Nation"

Positionspapier

2025

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

Ziele und Forderungen

Deutschland und Europa müssen angemessen und souverän die digitale Zukunft gestalten können. Das ist im Zeichen der aktuellen geopolitischen Lage drängender als jemals zuvor. 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, um unsere Bürgerinnen und Bürger, Unternehmen, Behörden und kritischen Infrastrukturen in angemessener Weise zu schützen. Dies betrifft insbesondere Kommunikation, Kooperation und Koordination auf Basis gemeinsamer Grundwerte.

In diesem Kontext hat die 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, mutig und gemeinsam 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, 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 insbesondere an die politischen Stakeholder:

Cyber-Sicherheit auf die Agenda heben **heißt:**

Bei allen Stakeholdern muss das Bewusstsein für die Bedeutung der Cyber-Sicherheit geschaffen werden. Politisch heißt das insbesondere:

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

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

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

[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

***Cyber-Resilienz signifikant erhöhen* heißt:**

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

***Technologiekompetenz gezielt nutzen* und *einen florierenden Cyber-Markt Deutschland aufbauen (bzw. weiter ausbauen und stärken)* heißt:**

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

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

***Cyber-Sicherheit pragmatisch gestalten* heißt:**

7. **Cyber-Sicherheit muss konsequent bereits beim Design neuer Dienste und Architekturen mitgedacht werden und selbst digital werden. Gleichzeitig ist immer wieder die richtige Balance aus Sicherheit, Nutzerfreundlichkeit und möglichst nahtloser Integration zu finden.**

8. **Klares Bekenntnis zu unbeschränkter/umfänglich wirksamer IT-Sicherheit**

Forderung: Bund und Länder müssen sich stärker zur IT-Sicherheit bekennen, deren Umsetzung vorantreiben und entsprechende Investitionen tätigen. Sie sind gefordert, bei der Implementierung von Cyber-Sicherheitsmaßnahmen eine Vorreiterrolle für alle weiteren Stakeholder einzunehmen und sollten in diesem Kontext mehr Zentralisierung und weniger Fragmentierung in der Cyber-Sicherheit ermöglichen.

Hintergrund: Die fortschreitende Digitalisierung ist die Basis für das Wohlergehen unserer modernen Gesellschaft und eröffnet über alle Branchen und Unternehmensgrößen hinweg enorme Wachstumschancen. Der Digitalisierungsprozess beschleunigt auf allen Ebenen, der digitale Anteil in nahezu allen Produkten und Lösungen steigt kontinuierlich. Mit der zunehmenden Durchdringung der Digitalisierung nimmt auch die Fähigkeit ab, analoge Prozesse wieder aufzunehmen. Gleichzeitig nehmen die IT-Sicherheitsprobleme zu, weil die IT zur Zeit noch nicht sicher genug konzipiert und aufgebaut ist, um intelligenten Angriffen von Hackern erfolgreich entgegenzuwirken.

Daher ist eine umfänglich wirksame IT-Sicherheit die Voraussetzung für einen hohen Grad an Privatsphäre, den besonderen Schutz der Unternehmenswerte und für werteorientierte IT und IT-Dienste und somit für eine hohe Akzeptanz der digitalen Zukunft. Digitalisierung und generell alle technischen Innovationen brauchen Vertrauen als Basis einer breiten Akzeptanz. Wenn diese Technologien aber nicht sicher betrieben werden können, dann wird das Vertrauen zunächst in einzelne Technologien zerstört und nach und nach entsteht ein technologiekritisches Klima.

IT-Sicherheit sollte Informationssicherheit mit allen Schutzzielen (Vertraulichkeit, Integrität, Verfügbarkeit) beinhalten und nicht nur rein technische Schutzmaßnahmen berücksichtigen.

Der Bund und die Länder haben sich endlich klar und unverrückbar zur umfassenden IT-Sicherheit zu bekennen und ihr Verhalten danach auszurichten. Eine passende Werteorientierung zum Aufbau und Erhalt von Vertrauen von Unternehmen und Bürgerinnen und Bürgern ist dafür wesentlich.

9. **Europäische IT-Sicherheitsgesetze für eine erhöhte Rechts- und Investitionssicherheit - klar, konsolidiert und agil**

Forderung: 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.

Hintergrund: Die Gesetze mit Bezügen zur IT-Sicherheit sind dringend auf den Prüfstand zu stellen. Sie sind erkennbar und konsequent an der Steigerung der IT-Sicherheit, der technologischen und digitalen Souveränität Deutschlands und der EU und vor allem der Wahrung der Grundrechte und Grundwerte unserer Verfassung auszurichten.

Der Anwendungsbereich des nationalen IT-Sicherheitsgesetzes sollte auf den Mittelstand erweitert werden, da die Risiken im Rahmen der IT-Sicherheit alle Unternehmen und nicht nur die Betreiber Kritischer Infrastrukturen sowie deren Zulieferer betreffen. Die Anforderungen sind so zu gestalten, dass sie von allen Stakeholdern, insbesondere also Unternehmen und Behörden, dauerhaft leistbar sind.

Die Gesetze sind so aufeinander abzustimmen, dass Unklarheiten minimiert und die Rechtssicherheit maximiert wird. Dies betrifft nationale Gesetze untereinander und nationale Gesetze im Verhältnis zu europäischen Verordnungen. Es gibt beispielsweise keine systematische Abstimmung von Anforderungen an den Stand der Technik, obwohl dieser im BSIG, TMG, TKG, der DSGVO u.a. Gesetzen mehrfach verwendet wird. Das betrifft mittelbar auch Gesetze wie das GeschGehG, die Geheimhaltungsmaßnahmen fordern, aber keinen Bezug zu einem Technologieniveau aufweisen.

Die unsystematische IT-Sicherheitsgesetzgebung wirkt auch auf der Ebene der Tätigkeit der Aufsichtsbehörden fort. Trotz ein und derselben Materie gibt es hier massive praktische, rechtliche, technische und wirtschaftliche Unsicherheiten, die deutlich verringert werden sollten.

IT-Sicherheitsgesetze sollten künftig weitestgehend auf Ebene der Europäischen Union geregelt werden. Die Gesetze sind der Natur des Regelungsgegenstandes wegen möglichst agil zu gestalten. Es sollte ein Benchmarking entwickelt werden, mittels dessen die Wirkmächtigkeit der IT-Sicherheitsgesetze nachvollziehbar geprüft werden kann. In den jeweiligen Gesetzgebungsverfahren sind die Fachkreise rechtzeitig, nachhaltig und ernsthaft einzubeziehen. Das war zuletzt beim IT-Sicherheitsgesetz 2.0, der TKG-Novelle u. a. nicht der Fall.

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

Forderung: 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 einer staatlich motivierten 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.

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

Forderungen:

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 muss 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 KMU 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. Branchenspezifische nationale Systeme müssen unter Berücksichtigung der europäischen Vorgaben zusammengeführt werden.

Resilienz erhöhen - Angesichts der aktuellen Cyberbedrohungslage müssen wir IT-Infrastrukturen deutlich robuster aufstellen und insbesondere Kritische Infrastrukturen auch bei Cyberangriffen lauffähig halten.

Der Weltraum ist ebenfalls Kritische Infrastruktur - Die Bundesregierung sollte sich für ein generell hohes Schutzniveau auch von Weltraumsystemen einsetzen.

Hintergrund: Eine Erhöhung der Resilienz gegen Cyberattacken betrifft gleichermaßen Bürgerinnen und Bürger, Wirtschaft und Verwaltung. Grundsätzlich ist ein flächendeckender und ganzheitlich ausgelegter Schutz aller genannter Zielgruppen nach dem Stand der Technik zu erreichen. Dabei sind neben querschnittlichen Themen und Maßnahmen auch zielgruppenspezifische Umsetzungsmaßnahmen zu treffen.

Geschäftsprozesse lassen sich längst vollumfänglich digitalisieren und auch bei Remote-Work ist eine hohe IT-Sicherheit durch vertrauenswürdige Lösungen möglich. Um ganzheitliche Sicherheit für Wirtschaft und Gesellschaft zu gewährleisten, braucht es aber neben einer deutlichen Erhöhung der allgemeinen Awareness auch politisch-regulatorische Maßnahmen. Der Aufbau von IT-Sicherheitsinfrastrukturen kann entlang der folgenden Themenfelder gelingen.

12. Gesetzliche Rahmenbedingungen schaffen

Forderungen:

Zügige Umsetzung des NIS-2-Umsetzungs- und Cyber-Sicherheitsstärkungsgesetzes - Die Europäische NIS-2 Richtlinie soll die Resilienz Kritischer Infrastrukturen und der zugehörigen Lieferkette stärken und definiert hierzu ein Bündel an Cyber-Sicherheitsmaßnahmen. Die zeitnahe Transformation in deutsches Recht unterstützt das Vertrauen in deutsche Unternehmen und die deutsche Kritische Infrastruktur und stärkt damit die Wettbewerbsfähigkeit deutscher Unternehmen im internationalen Umfeld.

In gleichem Maße müssen sich deutsche Unternehmen auf die Services ihrer Kommunen und Gemeinden verlassen können. Daher ist eine zeitnahe Umsetzung der NIS2-Anforderungen nicht nur auf Bundes- sondern auch auf Landes- und Kommunalebene unumgänglich. Die Unterstützung der Unternehmen und Behörden durch das BSI ist hierbei besonders wichtig. Dies kann insbesondere durch den Ausbau des BSI zur Zentralstelle und durch zusätzliche Stellen gefördert werden. Die gezielte Einbindung der Cyber-Sicherheitsindustrie würde das BSI bei diesen Aufgaben entlasten und Behörden und Unternehmen bei Implementierung und Zertifizierung der geforderten Maßnahmen zusätzlich unterstützen.

Produktsicherheit stärken und incentivieren - Der Cyber Resilience Act (CRA) trat am 11.12.2024 in Kraft. Hersteller sind ab 11.09.2026 aufgefordert, darin enthaltene und öffentlich gemachte Schwachstellen zu melden und ab Dezember 2027 verpflichtet, ihre Produkte cybersicher zu entwickeln. Dadurch entsteht eine weltweite Gleichbehandlung aller Hersteller, die ihre Produkte in Europa verkaufen möchten. Die Bundesregierung ist nun aufgefordert, die Hersteller bei der Umsetzung der Maßnahmen zu unterstützen. Speziell KMU und Start-Ups benötigen hierbei Unterstützung. Bspw. geförderte Unterstützungsleistungen durch die Cyber-Sicherheitsindustrie sowie Steuererleichterungen bei frühzeitiger Implementierung von Cyber-Sicherheitsmaßnahmen in deren Produkte sowie rund um die Zertifizierung würden den Prozess erheblich beschleunigen und damit das Angebot cybersicherer Produkte in den Segmenten Energie, Industrie, Pharmazie, Wasser/Abwasser, Weltraum, Privathaushalte, etc., frühzeitig erhöhen.

Nicht nur die Wettbewerbsfähigkeit deutscher Hersteller, auch die Betreiber Kritischer Infrastrukturen und die Bürger würden von der Verfügbarkeit cybersicherer Produkte maßgeblich profitieren. Gleichzeitig stärkt dies auch das Vertrauen in die Digitalisierung und damit deren Nutzung.

Es sind klare Vorgaben zu schaffen, wie die Resilienz in Deutschland einheitlich gemessen werden kann. Einheitliche Bewertungsgrundlagen und Benchmarks sind bereitzustellen, um darauf basierend - in Abstimmung mit Unternehmen - Best Practices für Cyber-Resilienz zu entwickeln, gegebenenfalls unter Berücksichtigung der spezifischen Anforderungen von kleinen, mittleren und großen Unternehmen. Ein solcher Best-Practice-Katalog ermöglicht es insbesondere KMU mit begrenzten Cyber-Sicherheitsressourcen, geeignete Lösungen effizient zu identifizieren und zielgerichtet umzusetzen.

Darüber hinaus ist ein umfassendes Gesamtpaket zu entwickeln, das sowohl den aktuellen Resilienzstatus ermittelt als auch geeignete Maßnahmen definiert. Dieses Paket sollte in Zusammenarbeit mit der Versicherungsbranche gestaltet werden, um Unternehmen Zugang zu Cyber-Versicherungen zu ermöglichen, die neben der Abdeckung von Schadenskosten auch die Unterstützung durch Incident-Response-Dienstleister im Ernstfall sicherstellen.

Besondere Bedeutung kommt der verpflichtenden Erstellung eines Incident-Response-Plans zu, da hier in Deutschland ein erheblicher Nachholbedarf besteht. Zur Unterstützung der KMU sind praxisorientierte Templates, Hilfestellungen bei der Implementierung sowie regelmäßige Wiederholungstrainings bereitzustellen.

Vertrauenswürdige digitale Identität als Basis - Eine sichere und vertrauenswürdige Identifizierung ist die notwendige Voraussetzung für die Verlagerung von Geschäftsprozessen in die Online-Welt und ist damit eine wesentliche Basis für alle Ziele der Initiative der Cyber-Nation. Hierfür müssen die notwendigen gesetzlichen Rahmenbedingungen geschaffen werden, damit vertrauenswürdige Identitäten für natürliche und juristische Personen einfach, interoperabel, grenzüberschreitend und sicher genutzt werden können.

Auf EU-Ebene hat die Europäische Kommission mit dem vorgeschlagenen Rahmen für eine europäische digitale Identität die Möglichkeit eröffnet, sich mit einer digitalen Brieftasche (European Digital Identity Wallet - EUDIW) sicher und benutzerfreundlich zu identifizieren oder andere digitale Nachweise vorzulegen. Diese Initiative sollte zügig im Rahmen der vorgegebenen europaweiten Zeitpläne zum Abschluss gebracht und EU-weit umgesetzt werden.

Die europäischen Vorgaben zu einem gemeinsamen Identitätsökosystem müssen dafür schnell festgelegt und standardisiert werden. Die unterschiedlichen branchenspezifischen Systeme müssen zusammengelegt werden. Basis einer breiten Akzeptanz eines solchen Identitätsökosystems ist in jedem Falle ein grundlegendes Vertrauen. Die Beispiele DE-Mail, Personalausweis oder tagesaktuell die elektronische Patientenakte zeigen, dass dies nicht gelingt, wenn nicht eine ganzheitliche Betrachtung der Cyber-Sicherheit und weiterer regulatorischer Vorgaben (wie etwa Datenschutz) unter Einbeziehung aller Stakeholder (insbesondere auch der Zivilgesellschaft) erfolgt. In diesem Sinne ist etwa der im Jahr 2024 gestartete Konsultationsprozess zur deutschen Umsetzung der EUDIW als positives Beispiel zu nennen, der als Blaupause auch für andere Umsetzungsprojekte dienen kann.

(Ultra)Mobiles Arbeiten/Home Office - Die Corona-Pandemie hat auch in Deutschland den Trend zum (ultra)mobilen Arbeiten deutlich beschleunigt und zu einem de-facto-Standard in der aktuellen Arbeitswelt ausgeprägt. Das heißt insbesondere, dass es zu einer zunehmenden Ablösung der klassischen "Arbeitsplatzdefinition" von den genutzten IT-Systemen kommt. Insbesondere heißt dies auch, dass der Zugriff zu Datenbeständen, sei es, dass diese in dedizierten Unternehmensressourcen oder aber auch in Cloudsystemen vorliegen, konsequent immer auch mobil zu jeder Zeit und an jedem Ort möglich sein muss.

Auch der Einsatz von qualifizierten Vertrauensdiensten gemäß der eIDAS Verordnung und die konsequente Integration der Konzepte der EUDIW können hier wesentlich zur Erhöhung der Sicherheit und Vertrauenswürdigkeit beitragen.

Ziel muss es sein, diese qualifizierten Vertrauensdienste dabei breit in die Anwendung zu bringen. Dies ist nur zu erreichen, wenn gesetzliche Lücken geschlossen werden. Notwendig ist eine kohärente nationalgesetzliche Berücksichtigung der Vertrauensdienste, etwa in den E-Government-Gesetzen des Bundes und der Länder, in der Verwaltungsgerichtsordnung und dem BGB. Nur so werden sichere digitale und standardisierte Kommunikationsprozesse flächendeckend ermöglicht und tragen somit zu einer signifikanten Erhöhung der Cyber-Resilienz bei.

Absicherung von Organisationsidentitäten, Schutz vor Desinformation und Manipulation - Webseiten (und damit Organisationsidentitäten) werden immer wieder gefälscht, um Verbraucherinnen und Verbraucher in die Irre zu führen oder um sie dazu zu bewegen, vertrauliche Informationen wie Bankkontodaten preiszugeben. Um dies zu verhindern, sieht die eIDAS-Verordnung von 2014 sog. qualifizierte Website-Zertifikate (QWACs) vor, die drei Sicherheitsstufen kennzeichnen und von qualifizierten Vertrauensdiensteanbietern ausgestellt werden. Die in Art. 45 vorgesehene Regelung zur Anerkennung von QWACs und deren Anzeige ist ein Meilenstein für den Daten- und Verbraucherschutz und muss daher - wie die gesamte Gesetzgebung der Europäischen Kommission für eine EUDIW - zügig umgesetzt werden.

Dies gilt umso mehr, als Webseiten von Unternehmen, staatlichen Stellen und der Politik manipuliert und mit dem Ziel der Desinformation verfälscht werden. Auch gegen diese Gefährdungen ist eine konsequente technische Absicherung durch etwa die oben genannten Maßnahmen erforderlich.

E-Mail-Verschlüsselung bei Geschäftsprozessen - Nach wie vor besteht Aufholbedarf im Bereich der E-Mail-Verschlüsselung in der Wirtschaft, insbesondere bei KMU. Die Ursachen hierfür sind vielfältig.

Die Zukunft der sicheren und vertrauenswürdigen E-Mail-Kommunikation liegt in der verschlüsselten Übertragung. Die Technik hierfür ist etabliert. Explizite - sektor-/branchenspezifische - Verschlüsselungspflichten oder zumindest Verschlüsselungsempfehlungen würden für deren breitere Anwendung sorgen.

Für Unternehmen und Verwaltung ist E-Mail heutzutage allerdings nur ein Dienst unter vielen, der durch Verschlüsselung geschützt werden muss. Dieser Schutz muss bereits in der verwendeten Kommunikationsinfrastruktur, etwa beim (ultra-)mobilen Arbeiten, geschehen. Als Kommunikationsdienst wird E-Mail zudem zunehmend durch Messenger-Dienste abgelöst. Hauptproblematik bildet dabei der Übergang zwischen beruflich und privat genutzter Kommunikation, für den geeignete IT-Sicherheitslösungen bereits durch die Provider bereitgestellt werden müssen.

Staat als "Enabler" und "Ankerkunde" - Die E-Mail-Verschlüsselung wird sowohl von der Wirtschaft als auch im privaten Bereich nach wie vor viel zu selten genutzt. Vor diesem Hintergrund wäre zu überlegen, ob nicht weitere Maßnahmen notwendig wären, um die Nutzung dieser "Werkzeuge" "in die Fläche" zu bringen und damit für eine wirklich sichere IT-Sicherheitsinfrastruktur zu sorgen. Wünschenswert ist, dass alle Bürgerinnen und Bürger Verschlüsselungszertifikate erhalten. Ebenso könnte eine Ausgabe von QWACs zumindest im Public Sector an die entsprechenden Organisationen erfolgen. Dies ließe sich auch mit Projekten wie dem Bürgerservicekonto oder dem Unternehmenskonto als Plattformen zur Verteilung koppeln.

Durch seine Beschaffungsmacht hat der Staat erhebliche Möglichkeiten zur Beeinflussung der genutzten IT-Sicherheitsinfrastrukturen. Bereits die nationale Sicherheitsstrategie und die nationale Cyber-Sicherheitsstrategie sehen vor, den Staat in seiner Rolle als Ankerkunde für vertrauenswürdige Technologien zu stärken, um so gezielt die umfangreich in IT investierten öffentlichen Mittel zu kanalisieren und zur Steigerung der digitalen Souveränität zu nutzen. Hier kann der Staat gerade im Bereich von Sicherheitstechnologien von seinen vergaberechtlichen Möglichkeiten Gebrauch machen und gerade bei großen Infrastrukturprojekten auf Anbieter setzen, deren Vertrauenswürdigkeit überprüfbar ist und bei denen sich Wertschöpfung und Innovationsleistung im europäischen und deutschen Rechtsraum vollzieht.

IT-Sicherheit von Weltraumsystemen - Durch die hohe Kritikalität von Weltraumsystemen auf unsere Gesellschaft, sei es auf behördlicher, militärischer oder kommerzieller Ebene, ist der Weltraum als Kritische Infrastruktur mit äußerst hohen Auswirkungen im Falle erfolgreicher Cyber-Angriffe zu betrachten. Satelliten-Kommunikationsnetze wie IRIS² werden nicht nur von Behörden und Streitkräften benutzt werden, sondern dienen auch der kommerziellen Nutzung. Da dies auch für viele andere Satellitenanwendungen gilt, sollte sich die Bundesregierung für ein grundsätzlich hohes Schutzniveau einsetzen.

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

Forderung: Es ist essenziell, die technologische Souveränität zu stärken, indem Schlüsselkompetenzen entwickelt, Abhängigkeiten (insbesondere geopolitisch bedingte) 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. Bestehende Flickenteppiche müssen durch integrierte Lösungen ersetzt werden.

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.

Hintergrund: Die technologische Souveränität ist ein immer wichtiger werdender Faktor, weil in Zukunft in allen Branchen der Wertschöpfungsanteil von IT, dem Internet und der Daten zunehmen wird. Um die Gestaltungsmöglichkeiten unserer Gesellschaft auszuschöpfen, müssen alle Stakeholder wie Hersteller und Anwender von IT-Technologie sowie Wissenschaft, Politik und Verwaltung aus diesem Bereich gemeinsame Ziele definieren und umsetzen. Erforderlich ist ein gezielter Kompetenzaufbau in Schlüsselbereichen, um mögliche Risiken, die durch Abhängigkeiten entstehen (Hersteller, Herkunftsland, Einsatz, Wechselwirkungen), beurteilen zu können.

Generell sehen sich alle Stakeholder mit einer kontinuierlich steigenden Anzahl an Anforderungen konfrontiert. Dies betrifft insbesondere Anforderungen an die (Netzwerk)Infrastruktur von Unternehmen, staatlichen Organisationen, Kommunen und Städten. Eine Vielzahl von Software- und Hardware-Komponenten müssen miteinander funktionieren, verwaltet und gepflegt werden. Mit der Komplexität der IT-Infrastruktur nehmen sowohl die Administrations-, Anschaffungs- und Wartungskosten aber auch die Anfälligkeit und die Gefahr für Sicherheitslücken oder Ausfälle zu. Durch IT-Systeme eingegangene Abhängigkeiten sind dabei nur schwer und mit hohen Aufwänden rückgängig zu machen. Deshalb müssen sie ebenso als Risiken identifiziert und behandelt werden wie kritische Abhängigkeiten in anderen Bereichen, zum Beispiel bei Lieferketten und Energieversorgung.

Bekanntlich ist eine Kette nur so stark wie ihr schwächstes Glied. Das gilt besonders auch für IT-Infrastrukturen. IT-Sicherheit und Resilienz erlauben daher keine Kompromisse**.** Eine IT-Infrastruktur muss immer ganzheitlich konzipiert werden.

Dazu müssen wir weg vom architekturellen Flickenteppich der jetzt vorhandenen verschiedenen Cybersecurity Lösungen, hin zu einer ganzheitlich durchdachten IT-Infrastruktur, die alle Infrastruktur-Anforderungen erfasst. Nur so kann die Komplexität der Infrastruktur reduziert und können die Risiken minimiert werden.

Ziel muss es sein, einen Schutzschirm für die gesamte IT-Infrastruktur gegenüber unerwünschten Einflüssen von außen- und innen sicherzustellen, der Business Continuity, aber auch Flexibilität und Skalierbarkeit für zukünftiges Wachstum oder Veränderungen ermöglicht.

Besondere Aufmerksamkeit kommt hier beim Endgerät bzw. Der Infrastruktur des Anwenders zu, die insbesondere im (ultra)mobilen Arbeiten (s.u.) typischerweise nicht mehr vollständig in der Kontrolle des Arbeitgebers ist. Dies unterstreicht die Bedeutung und Notwendigkeit einer Absicherung der Infrastruktur auf dem Stand der Technik, insbesondere auf der Ebene der (End)Anwender.

Eine hochsichere Kommunikation muss das Ineinandergreifen aller Sicherheitselemente über die gesamte Kommunikationsstrecke beinhalten und die Schwachstellen an jeder dieser Schnittstellen beseitigen. Vom Anwender und seinem Rechner, über die gesamte Kommunikationsstrecke und auch innerhalb des zu schützenden Netzwerks.

Insbesondere für kritische Bereiche müssen wir alternative Schlüsseltechnologien entwickeln bzw. bestehende Technologien erweitern, um Abhängigkeiten zu reduzieren und den Einsatz vorhandener Technologien beherrschbar zu gestalten. Regulierungen müssen Vorgaben für den Einsatz von Technologien mit hohem Risikopotenzial für sicherheitskritische Bereiche setzen. Es müssen Prüfverfahren und -techniken für eine kontinuierliche Zertifizierung geschaffen werden, um einen beherrschbaren Einsatz sicherheitskritischer Technologien zu ermöglichen, insbesondere von außereuropäischen Anbietern.

Bei Open-Source-Software-Projekten (und natürlich auch bei Software-Projekten generell) sollte ein besonderer Schwerpunkt auf die Verifizierung der Softwarequalität, Sicherheit und Vertrauenswürdigkeit gelegt werden. Aber auch eine intensivere Beteiligung an der Entwicklung von internationalen Standards, um frühzeitig mitgestalten zu können, ist ein weiterer Aspekt, der von der Politik angestoßen und für wichtige Bereiche umgesetzt werden muss.

Im Bereich der IT-Sicherheit müssen wir "IT Security made in Germany/made in EU" zu Vertrauenssiegeln machen. Wir brauchen sichere und vertrauenswürdige KI-Systeme, die unsere Werteorientierung erfüllen und den Nutzer unterstützen und nicht zum Produkt machen. Wir brauchen sichere und vertrauenswürdige Hardwarekomponenten, die in allen verwendeten IT-Sicherheitssystemen den Schutz der Schlüssel gewährleisten und eine manipulationssichere Ausführungsumgebung der kryptografischen Algorithmen gewährleisten.

IT-Sicherheitsinfrastrukturen und deren Dienste wie zum Beispiel für VPN, E-Mail-Verschlüsselung, elektronische Identitäten und Nachweise für Nutzer und IT-Geräte (IoT, Industrie 4.0, Fahrzeuge, etc.), Domänenzertifikate usw. sollten mit Blick auf die Herkunft von Technologien und Produkten und zur größtmöglichen Harmonisierung im digitalen Binnenmarkt in europäischer Verantwortung liegen und den Stand der Technik erfüllen. Dabei sollte der Staat als wichtiger Ankerkunde auch darauf achten, dass er gerade bei identifizierten Schlüsseltechnologien der proklamierten Forderung nach vertrauenswürdiger Provenienz der genutzten Lösungen nachkommt.

Um Cloud-Angebote internationaler Anbieter nutzen zu können, müssen diese verpflichtet werden, nationale Sicherheitsanker und Technologien zur Absicherung der Services einzubinden. Es bleibt zudem sorgfältig zu prüfen, ob die derzeit diskutierten Marktmechanismen zur Erhöhung der Sicherheit und der digitalen Souveränität im Cloud-Umfeld ausreichend sind oder inwiefern diese nicht durch entsprechende nationale oder EU-weite Vorgaben, insbesondere ein EU-Cloud-Schema, zu ergänzen sind.

Wir müssen technologische IT-Sicherheit zum Schutz der Bürgerinnen und Bürger, der Wirtschaft und der Gesellschaft fördern und ausbauen, um Akzeptanz für die digitale Zukunft zu erreichen und deren langfristige Verfügbarkeit / Nutzbarkeit zu sichern.

Wie bereits oben erwähnt, ist es ein wichtiger erster Schritt, einen klaren Scope für Maßnahmen auf dem Weg zur Cyber-Nation zu definieren und hierbei auch zwischen querschnittlichen und den sektorspezifischen Maßnahmen zu unterscheiden, die sich in Summe zu einem ganzheitlichen Bild ergänzen.

14. Mehr und integral wirkende IT-Sicherheitstechnologie "Made in Germany" in der Praxis

Forderungen:

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 ortsansässige Unternehmen, KMU und junge Unternehmen bessere Erfolgsaussichten bei 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 Erarbeitung eines europäischen Cloud-Schemas und die aktuelle Cloudstrategie des BSI sollten 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.

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 der 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.

Hintergrund: Cloud-Plattformen als wichtige Basis - Wir sehen aktuell Schwierigkeiten, die sich mit der Machtkonzentration großer ausländischer Plattformbetreiber und dabei oft genutzter geschlossener Eco-Systeme für

- die Aufrechterhaltung einer für Deutschland essentiellen Unabhängigkeit der digitalen Verwaltung im Allgemeinen,
- dem Schutz sensibler Informationen (insbesondere VS-Kommunikation) im Speziellen,
- die unabhängige Erbringung kritischer Versorgungs-Dienstleistungen (KRITIS),
- als auch die uneingeschränkte Souveränität der volkswirtschaftlich bedeutsamen Produktion

ergeben könnten.

Innovative und hochwertige Komponenten sind hierzulande durchaus vorhanden, sie müssen aber noch deutlich stärker gefördert und bevorzugt eingesetzt und damit für die nationale Nutzung gesichert werden.

In einer Zeit, in der internationale Anbieter den Cloud-Markt dominieren, sehen sich deutsche Behörden und Unternehmen immer häufiger gezwungen, kritische Daten außerhalb ihrer Kontrolle zu speichern. Neben Skalierbarkeit und Effizienz rückt dabei die Datensouveränität in den Mittelpunkt. Europäische Organisationen müssen angesichts internationaler Gesetze wie dem US CLOUD Act ihre Daten sicher verwalten, ohne die Anforderungen der DSGVO zu gefährden.

Zur Wiedererlangung der technologischen und digitalen Souveränität sollten vorhandene Technologieproduktionen ausgebaut und Anreize für den Einsatz sicherer Systeme geschaffen werden. Ziel muss es dabei sein, Herstellungskompetenz für Schlüsselkomponenten im Sinne einer vertrauenswürdigen Eigenentwicklung und -produktion von IT-Sicherheitslösungen zu erlangen bzw. langfristig zu erhalten und nutzen zu können.

Aktuelle Vorhaben wie die Cloudstrategie des BSI weisen allerdings in eine entgegengesetzte Richtung und zielen eher darauf ab, auch im Verschlusssachenbereich Lösungen internationaler Anbieter ohne Sicherheitsanker vertrauenswürdiger Anbieter zu nutzen. Dies widerspricht der Vision von digitaler Souveränität einer Cyber-Nation Deutschland. Daher sollte die Cloudstrategie des BSI entsprechend überarbeitet werden und die Bundesregierung sich für die Aufstellung eines europäischen Cloudschemas zur Förderung europäischer Angebote einsetzen.

Im Sinne sicherer technischer Plattformen aus Deutschland und Europa sollten neben der Förderung von universitärer und industrieller Forschung erste industrielle produktive Deployments mit staatlichen Mitteln gefördert und genutzt werden. Dies betrifft sowohl die Hard- und Softwarekomponenten für komplette "Secure Platforms" (bzw. Netze aus solchen) als auch die europäischen Fähigkeiten in der Mikroelektronik, insbesondere CPU-Design und Herstellung. In diesem Zusammenhang ist die Schaffung von Standards und damit der Fähigkeit zur Interoperabilität unabdingbar. Die proklamierte "Halbleiter-Allianz" ist ein Schritt in die richtige Richtung und muss konsequent anwenderorientiert umgesetzt werden. Ein "Airbus-artiger" Umsetzungswille ist der Bedeutung angemessen.

Es muss die Bereitschaft und natürlich auch die Fähigkeit bestehen, nationale oder europäische schlagkräftige Industrie-Konsortien zu bilden. Dabei ist die Nutzung von Open Source Angeboten und damit verbundenen Entwicklungsmethoden ein wichtiges Element, um der Fragmentierung der Anbieterlandschaft zu begegnen und Synergien zu schaffen.

Nur eine strategische Entwicklung von technologischen Alternativen, Kompetenzerhaltung und -aufbau sowie eine auskömmliche Beschaffungspolitik und Verpflichtungen zum Einsatz der souverän betriebenen Plattformen ermöglichen nachhaltige Innovationsvorhaben für deutsche und europäische Schlüsseltechnologien. Der Erhalt hochqualifizierter Arbeitsplätze in diesem für Deutschland wichtigen Technologiefeld ist nur so möglich.

Die deutschen Unternehmen mit dem Schwerpunkt IT-Sicherheit sind fast ausschließlich große und mittlere Mittelständler sowie kleine und Kleinstunternehmen. Diese haben bei Ausschreibungen zur öffentlichen Beschaffung und zur Forschungsförderung jedoch in der Praxis kaum Zugang, da hierbei regelmäßig Anforderungen an etwa Alter, Umsatzvolumen und Unternehmensgröße gestellt werden, die sie nicht erfüllen können oder aber Unternehmen kein KMU im Sinne der Förderung sind, eigene umfangreiche Strukturen aber auch

nicht aufbauen können. Die rechtlichen Vorgaben für Vergabe und Forschungsförderung sollten dahingehend weiterentwickelt werden, dass sich bei Produkten und Dienstleistungen mit Bezug zur IT-Sicherheit lokale und junge Anbieter an solchen Ausschreibungen beteiligen können. Weiterhin sollten mittelständische und kleine, innovative Unternehmen aus dem Bereich IT-Sicherheit durch geeignete Förderung in die Lage versetzt werden, sich aktiv an Normungs- und Standardisierungsprozessen zu beteiligen.

Es müssen auf der Basis des IEC62443 oder NIST 800-82 insbesondere den KMU die Methoden, die Vorgehensweise eines OT-Assessments sowie deren Nutzen aufgezeigt werden. Die Risiken aus dem Bereich der OT sollen eng verknüpft mit den NIS-2 Anforderungen eruiert und dargestellt werden. Ebenso müssen die Zulieferer und die Supply Chain mit den für das Unternehmen kritischen Dritten/Zulieferern erfasst, nach Kritikalität eingestuft werden und mit geeigneten Maßnahmen abgesichert werden. Das BSI sollte hierfür auch regelmäßige Austausch Expertenrunden organisieren oder an z.B. TeleTrusT weiterreichen.

Zu "Made in Germany" gehört auch, dass alle deutschen Unternehmen ein angemessenes Augenmerk auf die eigene IT-Sicherheit legen. Mittleren, kleinen und Kleinstunternehmen einschließlich Start-ups bzw. Neugründungen fehlen jedoch meist die Finanzmittel, um IT-Sicherheit im eigenen Unternehmen konkret umzusetzen. Daher sollten auf die IT-Sicherheit fokussierte Fördermittel für bestehende Unternehmen (Entwicklungsförderung) und Start-ups (Gründungsförderung) bereitgestellt werden.

Zuletzt braucht es ein stärkeres Bewusstsein der Politik dafür, dass die IT-Sicherheitsbranche systemrelevant ist und Sicherheitskompetenz aus Deutschland und Europa zur Verfügung stehen muss. Die bedeutsamen Versorgungs- und Produktionsunternehmen sind in diesem Kontext als Nutzer einzubeziehen, um auch in Krisenzeiten durch die Aufrechterhaltung kritischer Dienstleistungen und der Produktion sowohl das staatliche Gemeinwesen als auch die Stabilität der Volkswirtschaft zu bewahren.

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. Solche Vereinbarungen sind auf konkrete Schutzbedarfe auszurichten und müssen prüfbare, detaillierte Leistungsangaben enthalten, die den Anwender in die Lage versetzen, die Erfüllung der gesetzlichen Vorgaben zu prüfen. Durch die sich ändernde Technik und das sich entwickelnde Recht sind diese Vereinbarungen komplex und sollten dennoch agil sein. Es ist wichtig, IT-Sicherheit nicht mehr in Form von Trivialanlagen zu verstehen, sondern als Grundlage von Ansprüchen auf eine bestimmte IT-Sicherheit. IT-Sicherheitsvereinbarungen sind wesentlicher Schutzschild digitaler Leistungen und unserer IT-Infrastrukturen - und haben selbst *state of the art* zu sein.

15. Cyber-Sicherheit pragmatisch gestalten

Forderung: Cyber-Sicherheit muss konsequent bereits beim Design neuer Dienste und Architekturen mitgedacht werden und im Sinne der Prozesse und Methodiken selbst digital werden. 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.

Hintergrund: 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.

Als Entsprechung zu Statik-Vorgaben und Umsetzungsüberprüfungen in der Architektur von Gebäuden sind in den Konzeptphasen für veränderte bzw. neue Architekturen von Produkten mit digitalen Elementen (sowie von Diensten, Anwendungen und Prozessen) verbindliche Sicherheits- und Datenschutzvorgaben zu identifizieren und in gebotener Kürze zu dokumentieren. Diese Cyber-Sicherheitsvorgaben sind aus jeweils mit allen Stakeholdern gemeinsam durchgeführten Bedrohungsanalysen abzuleiten und über den gesamten weiteren Lebenszyklus nachvollziehbar zu überprüfen und anzupassen.

Es muss immer klar sein: Cyber-Sicherheit soll bestehende und neue Anwendungen auf dem Stand der Technik absichern, ohne aber die eigentlichen Aufgaben und Ziele der Anwendungen zu behindern. Nur so kann eine breite Akzeptanz für den Einsatz von Cyber-Sicherheitsmaßnahmen geschaffen werden.

Absolute Sicherheit kann es nicht geben, das gilt insbesondere auch im Kontext der Cyber-Sicherheit. Diese pragmatisch zu gestalten, heißt damit auch immer: Risiken sind zu identifizieren und zu bewerten, es werden

aber immer Restrisiken verbleiben. Hier heißt es dann auch, diese eventuell auch in der entsprechenden Verantwortung zu akzeptieren, um zu verhindern, dass die Nutzerfreundlichkeit auf den "letzten Metern" doch wieder deutlich eingeschränkt wird.

Cyber-Sicherheit pragmatisch gestalten, heißt aber auch: Nachweise und Prüfungen zu vereinheitlichen und gute Standards wechselseitig und vollständig anzuerkennen (z.B. IT-Grundschutz Zertifikat mit ggf. speziellen fachlichen Bausteinen als vollständigen Ersatz für eine NIS2/§8a-Prüfungen oder C5:2020). Dies wäre eine deutliche Stärkung der Wertigkeit des IT-Grundschutz und damit auch eine Möglichkeit zum Bürokratieabbau, Anerkennung der Bemühungen des Instituts und Kostenersparnis.

Zu einer pragmatischen Umsetzung von Cyber-Sicherheit gehört auch eine Digitalisierung des gesamten Cyber-Sicherheitsprozesses in Unternehmen und Verwaltung. Insbesondere das Informationssicherheitsmanagement sollte mit Hilfe geeigneter digitaler Werkzeuge komplett digitalisiert werden. Dies betrifft mit Blick auf den IT-Grundschutz vor allem auch die Weiterentwicklung von sogenannten Grundschutz-Tools hin zu allen Erfordernissen eines digitalen Risikomanagements.

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.