Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

TeleTrusT
IT-Sicherheitsagenda 2029

Forderungen an die Politik

Bundesverband IT-Sicherheit e. V. (TeleTrusT)

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 eine Vorreiterrolle einnimmt. Für die nächsten beiden Legislaturperioden des Deutschen Bundestages hat TeleTrusT deshalb mit seiner "IT-Sicherheitsagenda 2029" wichtige und dringende Forderungen aufgestellt.

Digitalisierung und Vernetzung der Wirtschaft, Verwaltung und Kritischen Infrastrukturen bieten Unternehmen gute Chancen, ihr Know-how in neue Technologien und Dienstleistungen umzusetzen. Andererseits erhöht dies die Abhängigkeit gegenüber Dienstanbietern von den Monopolisten aus den USA und Asien. Gleichzeitig steigt das Risiko, durch Fehlfunktionen, Manipulationen oder Sabotage, erhebliche Schäden zu erleiden. Als Träger von Spitzen-Know-how steht die deutsche Industrie zudem im Fokus der internationalen Wirtschaftsspionage und Cyberkriminalität.

Der Staat ist für die Rahmenbedingungen der Bereitstellung und Absicherung von für die Gesellschaft wichtigen Funktionen und Infrastrukturen verantwortlich. Im Zuge der zunehmenden Komplexität der Infrastrukturen bedarf es einer intensiven Zusammenarbeit von Politik, Verwaltung, Forschung und Industrie, um die technologische und digitale Souveränität herzustellen bzw. zu gewährleisten.

Technologische und digitale Souveränität kann nur durch ein zielgerichtetes und langfristiges Vorgehen erfolgreich umgesetzt werden. Derzeit existieren zu viele Einzelinitiativen, die kaum Wirkung zeigen. Es bedarf einer Umsetzungsstrategie, die Ziele definiert, Maßnahmen priorisiert und festlegt sowie eine Aufgabenverteilung zwischen Politik, Verwaltung, Hersteller- und Anwendungsunternehmen und Forschung vornimmt. Die Politik ist aufgerufen, den Startimpuls für die Umsetzungsstrategie zu setzen und sie langfristig zu unterstützen. Andere Staaten verfolgen bereits konsequent entsprechende Umsetzungspläne. Demzufolge müssen Deutschland und Europa ihre Konkurrenzfähigkeit gegenüber anderen Regionen neu erlangen und erhalten, um weitestgehend unabhängig die digitale Zukunft zu gestalten.

Zentrale Forderungen:

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit

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

3. Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern

4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis

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

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

1. Klares Bekenntnis zu unbeschränkter IT-Sicherheit

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 und der Wertschöpfungsanteil der IT in allen Produkten und Lösungen wird immer größer. Andererseits nehmen die IT-Sicherheitsprobleme zu, weil die IT zur Zeit noch nicht sicher genug konzipiert und aufgebaut ist, um immer ausgefeilteren Angriffen intelligenter Hackerinnen und Hackern erfolgreich entgegenzuwirken.

Daher ist unbeschränkte 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.

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.

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

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.

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 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" zum Qualitätssiegel machen. Wir brauchen sichere und vertrauenswürdige KI-Systeme, die unsere Werteorientierung erfüllen und den Nutzerinnen und Nutzern 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, Autos, etc.), Domänenzertifikate usw. sollten hinsichtlich der Herkunft von Technologien und Produkten in europäischer Verantwortung liegen und den Stand der Technik erfüllen. In der Digitalisierung werden immer mehr Vertrauensdienste auf der Basis von PKI- und Blockchain-Technologien aufgebaut.

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.

3. Auf- und Ausbau von IT-Sicherheitsinfrastrukturen für Bürger, Unternehmen und Verwaltung fordern und fördern

Mit der zunehmenden Digitalisierung gewinnen die Themen Sicherheit und Vertrauenswürdigkeit in der Online-Welt mehr und mehr an Bedeutung. Der Ausbruch der Corona-Pandemie hat die Wichtigkeit noch einmal unterstrichen. Immer mehr Menschen erledigen betriebliche Abläufe digital von zu Hause und mitunter von privaten Geräten aus.

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 politisch-regulatorische Maßnahmen. Der Aufbau von IT-Sicherheitsinfrastrukturen kann entlang der folgenden Themenfelder gelingen.

Weiterführung, Skalierung und Bündelung der eID-Initiativen

Eine sichere und vertrauenswürdige Identifizierung ist die notwendige Voraussetzung für die Verlagerung von Geschäftsprozessen in die Online-Welt. Hierfür müssen die notwendigen gesetzlichen Rahmenbedingungen geschaffen werden.

Auf EU-Ebene hat die Europäische Kommission mit dem vorgeschlagenen Rahmen für eine europäische digitale Identität (EUid) die Möglichkeit eröffnet, sich mit einer EUid-Brieftasche sicher und benutzerfreundlich zu identifizieren oder andere digitale Nachweise vorzulegen. Diese Initiative sollte zügig zum Abschluss gebracht und EU-weit umgesetzt werden.

Auf nationaler Ebene wurde bereits die Smart-eID eingeführt. Zugleich laufen verschiedene Projekte zum Thema Self-Sovereign Identity (SSI). Diese nationalen Vorhaben sowie die hierbei gewonnenen Erkenntnisse und Erfahrungen sollten bei den Verhandlungen zum Rahmen für eine EUid und bei dessen Umsetzung berücksichtigt werden. Nur so kann ein konsistenter national-europäischer Rahmen für sichere Identitäten und Nachweise im europäischen Markt geschaffen werden.

Mobiles Arbeiten/Home Office

Gerade in Zeiten des mobilen Arbeitens, aber auch generell für die "digitalisierte Welt" gilt: Eine der größten Herausforderungen ist das Einholen von Unterschriften für Verträge und Vereinbarungen, also die vertrauenswürdige Identifizierung von Personen und Organisationen. Trotz der 2014 in Kraft getretenen Verordnung für elektronische Identifizierung und Vertrauensdienste (eIDAS), die hierfür einen Rahmen geschaffen hat und trotz der eindeutigen Nutzenvorteile von eIDAS-Werkzeugen, wie der qualifizierten elektronischen Signatur und dem elektronischen Siegel, ist deren Einsatz noch stark ausbaufähig.

Ziel muss es sein, diese qualifizierten Vertrauensdienste 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.

Absicherung von Webseiten

Webseiten 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 sollte - wie der gesamte Vorschlag der Europäischen Kommission für eine EUid - zügig verabschiedet und umgesetzt werden.

E-Mail-Verschlüsselung bei Geschäftsprozessen

Nach wie vor besteht Aufholbedarf in Sachen 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.

Staat als "Enabler"

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.

4. Mehr IT-Sicherheitstechnologie "Made in Germany" in der Praxis

Die Politik nimmt eine Vorbildfunktion ein und kann mit ihrer regulatorischen Kompetenz einen Regelungsrahmen zur gezielten Förderung von IT-Sicherheit in Deutschland schaffen. Zur Wiedererlangung der technologischen und digitalen Souveränität sollten vorhandene Technologieproduktionen ausgebaut und Anreize für den Einsatz sicherer Systeme geschaffen werden.

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 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. 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.

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 sie nicht erfüllen 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 kleine, innovative Unternehmen aus dem Bereich IT-Sicherheit durch geeignete Förderung in die Lage versetzt werden, sich aktiv an Normungs- und Standardisierungsprozessen zu beteiligen.

Zu "made in Germany” gehört auch, dass alle deutschen Unternehmen ein angemessenes Augenmerk auf die eigene IT-Sicherheit legen. Mittlere, kleine 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.

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

Deutschland darf nicht durch gesetzliche Verpflichtungen oder auf anderen Wegen die Schwächung von IT und IT-Diensten veranlassen, wie bei der Nutzung des Bundestrojaners, 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 eine Absage erteilt werden.

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

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

Die Gesetze mit Bezügen zur IT-Sicherheit sind dringend auf den Prüfstand zu stellen. Sie haben sich 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. Es bedarf eines unerschütterlichen Bekenntnisses zum Recht Jedermanns auf Verschlüsselung ohne technische Backdoors des Staates.

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 den Unternehmen 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 mehr 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.

Die stark ausgeweiteten Befugnisse des Bundesamts für Sicherheit in der Informationstechnik (BSI) sind gesetzlich auf ein Maß zurückzuführen, das einer effektiven, prüfbaren und kompetenziell sinnvollen Zuordnung von Rechten und Pflichten der Behörde entspricht.

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.

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 Experten, 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 Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4310
Fax: +49 30 4005 4311
https://www.teletrust.de