TeleTrusT-Positionen

2018-01

Impressum

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

I Branchenpositionen

TeleTrusT hat seine Mitglieder, d.h. die organisierte IT-Sicherheitsbranche, befragt, welche IT-sicherheitsrelevanten Themen die Bundestagsparteien adressieren sollten. Das Ergebnis kennzeichnet die Problemlagen der IT-Sicherheit in Deutschland:

1. Digitale Souveränität: Die Bundesrepublik Deutschland darf ihre technologische Hoheit über kritische IT-Anwendungen nicht verlieren.
2. Es bedarf eines überparteilichen Konzeptes, wie Deutschland Unternehmen davor schützt, über die IT ausgespäht zu werden und Innovationen zu verlieren.
3. Die Nationale Cyber-Sicherheitsstrategie muss durch einen Nationalen Cyber-Umsetzungsplan flankiert werden.
4. Deutschland benötigt einen politischen Hauptansprechpartner für die Digitalisierung.
5. Die Nutzung von IT-Sicherheitstechnologie "made in Germany" muss bei Staat, KRITIS und volkswirtschaftlich wichtigen Produktionsunternehmen Präferenz haben.
6. Der deutsche Mittelstand ist bei der digitalen Transformation zu Industrie 4.0 auf politische Unterstützung angewiesen.
7. Digitalisierung darf nicht automatisch den Verlust der Hoheit über vertrauliche Daten bedeuten.
8. Datenschutz "made in Germany" muss ein international wettbewerbsrelevanter Standortfaktor sein.
9. Ohne digitale Verwaltung kann die Digitalisierung Deutschlands nicht gelingen.

10. Sichere elektronische Identitäten sind das Fundament der Digitalisierung von Staat, Wirtschaft und Gesellschaft.
11. Der Einsatz von elektronischen Signaturen muss gefördert werden.
12. Die Digitalisierung des Gesundheitswesens ist eine gesellschaftliche Aufgabe, bei der IT-Sicherheit an erster Stelle stehen muss.
13. Die Schutzbereiche des IT-Sicherheitsgesetzes sollten ausgeweitet werden.
14. Die haftungsrechtliche Verantwortung für Sicherheitsmängel bei digitalen Produkten und Dienstleistungen muss eindeutig geregelt werden.
15. Anwender müssen im digitalen Umfeld zum Einsatz von Kryptographie motiviert werden.
16. Mailverschlüsselung muss einfach und damit für alle nutzbar sein, d.h. Unterstützung eines deutschlandweit einheitlichen Angebotes.
17. "Bundestrojaner" sind abzulehnen.
18. Die Bundesregierung muss zu einem aktiven, orchestrierenden Part in der Cybersicherheit werden, dazu ihre Erkenntnisse über die Schutzqualität von (durch Bundesbehörden) getesteten Verfahren, Produkten, Dienstleistungen auch anderen, insbesondere Ländern und Kommunen, zur Verfügung stellen und mittelfristig einen Basisschutz bei allen öffentlichen Organisationen etablieren.
19. Die Konsolidierung der IT des Bundes mit Konsolidierung der IT-Sicherheit muss ein wichtiger Schritt in der aktuellen und kommenden Legislaturperiode sein.

Desweiteren:

- Ausbau und Erhalt der technologischen Souveränität bei Verschlüsselungstechnologie
- Awareness-Programme für Informationssicherheit für Unternehmen und Bevölkerung
- Förderung der Kooperation zwischen IT-Sicherheitsunternehmen und Wirtschaftsunternehmen bzw. Integratoren
- Förderung der Nutzung des elektronischen Personalausweises
- Förderung deutscher IT-Sicherheitsunternehmen und Unterstützung bei der Bildung von international wettbewerbsfähigen Marktteilnehmern
- Förderung von IT-Hochsicherheitslösungen
- Hauptaugenmerk auf IT-Sicherheit im Produktionsumfeld
- Herstellerverpflichtung zur IT-Sicherheit für IoT-Geräte durch entsprechende Normen und Rechtsvorschriften einschließlich der Möglichkeit von Verbotsverfügungen
- Internationale Verträge zur Ahndung von IT-Kriminalität, Stärkung der Exekutive
- Keine staatlichen Backdoors bei verschlüsselter Kommunikation
- Konsequente Umsetzung der EU-DSGVO
- Vergabepolitik in sensiblen Bereichen des Gemeinwesens mit Berücksichtigung nationaler Interessen
- Nutzung von eID und nPA für digitale Services im öffentlichen Bereich
- Schaffung von steuerlichen Anreizen für KMU zur Verbesserung des Niveaus der Informationssicherheit, da Förderinstrumente gerade für KMU nicht ausreichend oder zu komplex sind

- Schlüsselrolle des BSI für die nationale Informationssicherheitswirtschaft anerkennen und umsetzen
- Schutz der IT-Infrastrukturen auf Bundes-, Länder und Kommunalebene
- Sichere elektronische Identitäten, Zweifaktorauthentisierung, Unabhängigkeit der Vertrauensinfrastrukturen von nichteuropäischen Anbietern.

II TeleTrusT-Leitpositionen im Einzelnen

1. Insbesondere vertrauenswürdigere, robuste IT-Systeme, die die Probleme "Softwaresicherheit" und "Malwarebefall" adressieren, sollten gefördert werden. IT-Sicherheitslösungen sollten auf starker Kryptographie basieren und im Kern der IT-Systeme verankert sein. Proaktive IT-Sicherheitslösungen für "Industrie 4.0" sollen direkt umgesetzt werden und Deutschland damit eine weltweite Vorreiterrolle in IT-Sicherheit und Vertrauenswürdigkeit in Bezug auf die Leitindustrien übernehmen. Proaktive Lösungen - Sicherheitskerne in Kombination mit Virtualisierung - sind ein innovativer Lösungsansatz, zu dem in Deutschland starke nationale Kompetenz vorhanden ist.

2. Eine der zentralen Herausforderungen von Industrie 4.0 wird die Absicherung der vernetzten Automatisierungssysteme gegen Risiken aus dem unsicheren Internet sein: IT Security, Datenschutz und Safety müssen auf hohem Qualitätsniveau in deutschen Lösungen für Industrie 4.0 etabliert sein. Eine Kombination aus der Industriemarke "Made in Germany", deutschem Datenschutz und "IT Security made in Germany" (ITSMIG) kann zum neuen Qualitätszeichen werden und somit den Industriestandort und die Exportnation Deutschland im internationalen Vergleich stärken. TeleTrusT sieht in Industrie 4.0 große Chancen und fordert daher schnelles Handeln:

- Besondere Berücksichtigung von Security by Design, Privacy by Design und Safety by Design bei Planung und Entwicklung von Industrie 4.0;

- Förderung einer politischen Allianz zwischen deutscher IT-Sicherheitswirtschaft und deutschem Maschinenbau im Rahmen der Digitalen Agenda der Bundesregierung;
- Durchführung von Maßnahmen zur 'Awareness'-bildung und Schaffung gesetzlicher Rahmenbedingungen zur Umsetzung von IT-Sicherheit in 'Industrie 4.0';
- Stärkere Berücksichtigung von IT-Sicherheit und Safety in der Ausbildung von Ingenieuren auch im Maschinenbau.

3. Die rechtliche Verantwortung für IT-Lösungen sollte erhöht werden, um Hersteller und Dienstleister zu mehr IT-Sicherheit zu motivieren. Hersteller müssen Verantwortung übernehmen, um Vertrauen zu schaffen. Ein pragmatischer und ausgewogener Rechtsrahmen sollte dem Schutzbedürfnis der Anwender ebenso gerecht werden wie der unternehmerischen Risikokalkulation.

4. Mit Hilfe der "Allianz für Cybersicherheit" sollte eine zielgerichtete gemeinsame Verteidigungsstrategie im Internet umgesetzt werden. Dazu gehört in einem ersten Schritt ein geeignetes und gemeinsames Internet-Sicherheitslagebild. Außerdem sollten IT-Sicherheitskompetenzzentren mit unterschiedlichen Schwerpunkten kooperativ gebildet werden, um den Aufwand in der deutschen Industrie und in der Verwaltung zu reduzieren.

5. Zertifizierte Weiterbildung zu Themen der Informationssicherheit im wirtschaftlichen Umfeld sollte durch staatliche Anreize gefördert werden.

6. Staatliche Anreize sollten die Beschaffung und Abschreibung von Investitionen in Zukunftstechnologien fördern. Verbindliche Sicherheitsmindeststandards für Beschaffungen in der öffentlichen Verwaltung bei kritischen Infrastrukturen sollten das Thema IT-Sicherheit adressieren.

7. Die Sichtbarkeit deutscher Spitzentechnologie und deutscher Unternehmen in Bezug auf IT-Sicherheit sollte staatlich unterstützt werden.

8. Bei den Domänenzertifikaten in Deutschland sollte ein Marktanteil von mindestens 60 % insgesamt und 80 % bei den "Top 1.000"-Webseiten angestrebt werden.

9. Öffentliche Institutionen mit Verwaltungs-PKI sollten mit gutem Beispiel vorangehen und persönliche E-Mail-Zertifikate sowie flächendeckend Gruppenzertifikate über den Verzeichnisdienst der "European Bridge CA" öffentlich erreichbar machen.

10. Es sollten mindestens 20 % aller E-Mails in Deutschland end-to-end-verschlüsselt werden.

11. Ein gemeinsames Gremium mit Vertretern aus Politik, Anwendern, Wissenschaft und IT-Sicherheitsindustrie sollte eine "Roadmap IT-Sicherheit Deutschland" mit Handlungsempfehlungen für unterschiedliche Schutzbedarfe erarbeiten.

12. Für IT-sicherheitsbezogene Unternehmungen, Entwicklungen und Markterweiterungen sollte ein adäquater Risikokapitalmarkt gefördert werden.

13. In zukunftsorientierten Themenfeldern der Informationstechnologie sollte eine zielgerichtete und innovative IT-Sicherheitsförderung mit besonderem Fokus auf den Transfer der Ergebnisse in die Wirtschaft etabliert werden.

14. Angesichts der Gefahren von Big Data muss ein gesellschaftlicher Dialog darüber geführt werden, was bezüglich der Erzeugung und Auswertung von Daten künftig erwünscht und was unerwünscht ist. Basis der Überlegungen muss eine Chancen-/Risikenabwägung sein, wie sie auch in anderen Technologiebereichen stattfindet.

15. Wesentliche Grundlage der Energiewende ist die dezentrale Erzeugung und Verteilung von Elektrizität, die umfangreiche Maßnahmen zur intelligenten Steuerung erfordert. Eine der dafür notwendigen intelligenten Komponenten sind Smartmeter, die intelligenten digitalen Stromzähler, die u.a. auch dynamische Tarife ermöglichen. Um eine Integration bzw. Steuerung in intelligenten Energienetzen abzusichern, ist anspruchsvolle IT-Sicherheit nötig. Bisher wurden keine verbindlichen Standards veröffentlicht bzw. in die Gesetzgebung eingebracht. Dies behindert und verzögert den raschen Aufbau der für die Energiewende benötigten sicheren kritischen Infrastruktur. Schnelles Handeln aller Verantwortlichen ist notwendig, um die Versorgungssicherheit der deutschen Bevölkerung und der Industrie mit Elektrizität weiterhin zu gewährleisten.

16. Vor dem Hintergrund der fortdauernden Bemühungen, die Anwendungsmöglichkeiten des neuen Personalausweises bei gleichzeitiger höchstmöglicher Sicherheit zu verbessern, unterstützt TeleTrusT den Ansatz, die eID-

Funktion des nPA - die ein wichtiges IT-Sicherheitsfeature darstellt - als nicht-abschaltbar auszugestalten. Der nPA verkörpert in bester Weise eine IT-Sicherheitstechnologie, die weltweit ihresgleichen sucht, mit ausgereiften und pragmatischen IT-Sicherheitsmerkmalen, die im modernen Internet für eine höhere Sicherheit der Anbieter und Bürger sorgen. Das Problem der Passwörter, die als Authentifikationsverfahren genutzt werden, ist bekannt und die daraus resultierenden Schäden sind deutlich zu hoch. Mit zunehmender Wichtigkeit des Nutzungskontextes steigt das Risiko. Würde die eID-Funktion des nPA nicht-abschaltbar konfiguriert, würde das "Henne-Ei-Problem" reduziert und eine breitere Nutzung wahrscheinlicher. Aktuelle Forschungen, z.B. in Zusammenhang mit Onlinebanking und eMobility, betrachten den nPA bereits als in zukünftige IT-Sicherheitskonzepte eingebunden. Ebenso haben internationale Bestrebungen in diesem Bereich, wie z.B. die FIDO Alliance, die Vorteile der Nutzung für die verlässliche Identitätsverifikation erkannt und bemühen sich um deren Integration. TeleTrusT hat auf diesem Gebiet mit einigen Unternehmensmitgliedern einschlägige Aktivitäten erfolgreich umgesetzt und wird dies auch in Zukunft verfolgen. Aus Sicht von TeleTrusT könnte die nicht-abschaltbare eID-Funktion des nPA, verbunden mit einer Motivationskampagne für die nPA-Nutzung, das IT-Sicherheitsschadensrisiko für die Gesellschaft, für Unternehmen und Bürger, bedeutend reduzieren.

17. Die Diskussion bezüglich staatlicher Einflussnahme auf Verschlüsselung mag angesichts der aktuellen Bedrohungslage von der grundsätzlichen Motivation her zwar nachvollziehbar erscheinen, gleichwohl bedarf das Thema

"Verschlüsselung" der sorgfältigen Güter- und Interessenabwägung. Der Ansatz, bei Nutzung von Verschlüsselung dem Staat Schlüsselzugang gewähren, beachtet unzureichend die politische, rechtliche und technische Dimension. Derartige Erwägungen sind nicht zielführend. Die Politik sollte Konsultationsangebote der Fachleute nutzen. Aus Sicht von TeleTrusT stehen die politischen Forderungen im Gegensatz zur Absicht der "Digitalen Agenda" der Bundesregierung, Deutschland zum Verschlüsselungsstandort Nr. 1 zu entwickeln. Regelungen zur Schlüsselhinterlegung oder zur verpflichtenden Implementierung von Zugangsmöglichkeiten für Sicherheitsbehörden würden das Vertrauen in die IT-Wirtschaft und den Schutz durch staatliche Stellen erschüttern. Ohnehin würden dadurch lediglich bestehende, bislang vertrauenswürdige IT-Technologien und -Standards geschwächt, und es ist davon auszugehen, dass kriminelle oder terroristische Organisationen auf andere Möglichkeiten der Kommunikation ausweichen. Folge wäre eine flächendeckende Schwächung der Kryptolandschaft und der IT-Sicherheit. Eine Kryptoregulierung wäre für IT-Nutzer ein neuer zusätzlicher Hemmschuh auf dem Weg zum verantwortlichen Umgang mit den eigenen Daten. TeleTrusT hält eine Einschränkung von Verschlüsselung bzw. ein Verbot starker Verschlüsselung in der Praxis nicht durchführbar, nicht zweckmäßig und verfassungsrechtlich bedenklich. Eine Gesellschaft, die durch ihre freiheitliche, demokratische Verfassung auf die Eigenverantwortung des Einzelnen setzt, benötigt die Gewissheit, dass der Einzelne seine Privatsphäre wirksam schützen kann. Ungeachtet dessen muss sie darauf vertrauen können, dass auch die staatlichen Stellen ihrem verfassungsrechtlichen Auftrag zum Schutz der Grundrechte der Bürger hinreichend nachkommen.

18. TeleTrusT warnt davor, dass das Transatlantische Handels- und Investitionspartnerschaftsabkommen (TTIP) zu einer Absenkung der deutschen bzw. europäischen Datenschutz- und IT-Sicherheitsstandards führen könnte. TTIP beinhaltet den Ansatz, dass sich die Verhandlungsparteien auf Standards einigen werden, nach denen ein Marktzugang für Produkte und Dienstleistungen auch im IT-Bereich sichergestellt sein wird. Hieraus ergeben sich wichtige Impulse für die nationalen Vorgaben an IT-Sicherheitsprodukte. Das Thema IT-Sicherheit und im Besonderen das zentrale Element Kryptoalgorithmen sind in Bezug auf TTIP aufmerksam zu beobachten. Dies unter dem Aspekt, dass nationale Institutionen - wie z.B. in Deutschland das BSI - als Sachwalter hoher Standards nicht direkt in die Verhandlungen involviert ist, sondern ihre Vorstellung den Verhandlungsführern der EU-Kommission erst nahebringen müssen, um zu vermeiden, dass TTIP in diesem Zusammenhang durch amerikanische NIST-Standards geprägt wird. Wenn dies nicht mehr zu verhandeln wäre, würde es die gesamte deutsche IT-Sicherheitsindustrie betreffen. TeleTrusT geht von folgenden Prämissen aus und versteht sie als Handlungsaufforderung an die politischen Entscheidungs- und TTIP-Verhandlungsträge:

- Die ITK-Industrie profitiert von globalen Standards und globalen technischen Spezifikationen, aber die TTIP-Verhandlungen dürfen nicht im Wege politischer Zugeständnisse in eine Abwärtsspirale für IT-Sicherheitsstandards münden.
- TTIP darf in Bezug auf IT-Sicherheit nicht zu einem geringeren Sicherheitsniveau für kommerzielle IT-Produkte führen, insbesondere nicht zu schwächeren Kryptoalgorithmen.

- Grundsätzlich ist ein Handelsabkommen zwischen den USA und der EU zu begrüßen. Die Snowden-Affäre hat aber deutlich werden lassen, dass Europa sich nicht auf das grundsätzliche andere 'Privacy'-Verständnis der USA einlassen sollte.
- Bei Schaffung eines gemeinsamen Wirtschaftsraums ist zu erwarten, dass deutlich mehr Daten, insbesondere personenbezogene Daten, zwischen der EU und den USA hin- und herfließen werden. Dies darf nicht ohne abgestimmtes Datenschutzverständnis geschehen. Das Fehlen einheitlicher Standards würde ansonsten zu unterschiedlichen, wettbewerbsverzerrenden Anforderungen an Unternehmen dies- und jenseits des Atlantiks führen.
- Der liberalisierte Zugang zu öffentlichen Aufträgen darf die nationale digitale Souveränität nicht gefährden.

19. TeleTrusT begrüßt das "Gesetz zur Erhöhung der Sicherheit Informationstechnischer Systeme "("IT-Sicherheitsgesetz"). Gleichzeitig hält es TeleTrusT für erforderlich, das Gesetz nachzubessern und zu konkretisieren. Dass der Gesetzgeber einen Vorstoß mit dem Ziel unternommen hat, Defizite in der IT-Sicherheit abzubauen, ist positiv zu bewerten. Fast täglich zeigen Meldungen zu Sicherheitsvorfällen in Unternehmen und Behörden, dass auch in Deutschland dringender Handlungsbedarf zur Verbesserung der IT-Sicherheit besteht. In der verabschiedeten Form wird das Gesetz jedoch wenig zur Verbesserung der Sicherheitslage beitragen, da der Gesetzgeber

weder Bewertungskriterien für die sicherheitsrelevanten technischen und organisatorischen Vorkehrungen benannt, noch sonstige Vorgaben zu Mindestanforderungen aufgestellt hat. Das Verhältnis zum technischen Datenschutz ist ebenfalls unklar. Ferner werfen Ausgestaltung der Meldepflichten von IT-Sicherheitsvorfällen und die Befugnisse des BSI rechtliche und praktische Fragen auf. Die Unternehmen sehen sich vielen unbestimmten gesetzlichen Anforderungen ausgesetzt, die erhebliche Rechtsunsicherheit mit sich bringen. TeleTrusT wird sich daher dafür einsetzen, die bestehenden Lücken gemeinsam mit allen Akteuren anzugehen und für Unternehmen transparente und handhabbare Anforderungen zu gestalten.

20. TeleTrusT begrüßt das EuGH-Urteil zu "Safe Harbor". Europäischen Firmen, die auch weiterhin ihre personenbezogenen Daten ausschließlich in Deutschland oder der europäischen Union verarbeiten, wird mit dem Urteil der Rücken gestärkt. Initiativen wie das TeleTrusT-Qualitätszeichen "IT Security made in Germany" erhalten die Bestätigung, dass der Datenschutz ein hohes Gut ist, das nicht ausgehöhlt werden darf.

21. Nationale Kryptographie-Souveränität und europäische Harmonisierung sind kein Widerspruch. Das Thema "Digitale Souveränität" betrifft in Bezug auf Kryptographie nicht nur die Schlüsselerzeugung, sondern auch die Algo-

rithmenwahl, einschließlich Schlüssellängen. Nicht umsonst werden sogenannte Krypto-Kataloge unabhängig vom Einsatz in Qualifizierten Signaturen/eIDAS üblicherweise national festgelegt. Andererseits sind für den Bereich "eIDAS" EU-einheitliche Festlegungen sinnvoll. TeleTrusT unterstützt die Forderung nach einer EU-weiten Regelung. TeleTrusT weist darauf hin, dass die Querwirkungen von nationaler Krypto-Souveränität, Harmonisierung im eIDAS-Kontext und auch Zertifizierungsdetails für QSCDs beachtet werden müssen, da zertifizierte Produkte z.T. sowohl als QSCDs, aber gleichzeitig auch in anderen Anwendungen eingesetzt werden. Die Algorithmen bilden die sicherheitstechnische Basis für die darauf aufsetzenden und unter eIDAS (teil-)geregelten Services. Ohne ein einheitliches Verständnis zur Gültigkeit der Algorithmen ist eine rechtlich und technisch harmonisierte Umsetzung in Europa nur schwer vorstellbar. Um in der EU möglichst gleiche Voraussetzungen im digitalen Binnenmarkt zu ermöglichen, empfiehlt TeleTrusT die Erarbeitung von Durchführungsrechtsakten, die den entsprechenden technischen Normen, die bereits erarbeitet wurden, Geltung verschaffen.

22. Informationstechnik ist zum Wirtschaftsfaktor geworden. "Informationelle Selbstbestimmung" und "Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten" im Sinne des Volkszählungsurteils des Bundesverfassungsgerichts von 1983 sind dennoch keine Konzepte von gestern. Eine massenhafte, anlasslose Speicherung von Bewegungsdaten, Nutzungsdaten, Kommunikationsdaten, Konsumdaten, Vitaldaten und Verhaltensdaten ist bzw. wäre mit dem

gesellschaftspolitischen Konstrukt der freiheitlich-demokratischen Grundordnung nicht vereinbar. Niemand kann ausschließen, dass sich Rechtsstaaten in Unrechtsregime verwandeln und aufgrund heutiger Sorglosigkeit über technische Instrumente verfügen werden, die umfassenden Zugriff auf die Daten aller Bürger gewähren und in der Folge jegliche politische Opposition verhindern.

23. Künftig sollen Daten in die USA datenschutzkonform auf Basis der Vereinbarung "EU-US Privacy Shield" übermittelt werden dürfen. Unternehmen können sich nach Ansicht von TeleTrusT auf diesen "Schild" nicht verlassen. Inhalt der Vereinbarung soll insbesondere die Zusage der US-Regierung werden, den massenhaften Datenzugriff der US-Behörden auf das erforderliche Maß zu beschränken und entsprechende Schutzmechanismen zu etablieren. Eine Massendatenspeicherung solle ausgeschlossen sein. Europäische Aufsichtsbehörden sollen Beschwerden an das US-Handelsministerium und die FTC weiterleiten können. Für Beschwerden gegen den Zugriff von Regierungsbehörden werde ein neuer Ombudsmann geschaffen. Statt staatlicher Regeln zur Begrenzung des Datenzugriffs seitens der USA bleibt es bei einseitigen Absichtserklärungen. Statt eines wirksamen gerichtlichen Rechtsschutzes richten die USA lediglich "Kummerkästen" ein. Die Wahrung des europäischen Grundrechts auf Schutz personenbezogener Daten würde ein radikales Umdenken der USA beim Thema Datenschutz, insbesondere beim Zugriff der Geheimdienste, voraussetzen. Das ist aber nicht in Sicht. Dies zeigen nicht zuletzt auch die aktuellen Gesetzgebungsverfahren zum USA Freedom Act und dem Judicial Redress Act. Beide werden die vom

EuGH aufgezeigten Missstände nicht beseitigen. Die Annahme, die USA werden allein aufgrund des "Privacy Shield" das Datenschutzniveau angemessen anheben können, ist nicht vertretbar. Es hieße nicht weniger als den Europäern ein höheres Schutzniveau zu gewähren als den eigenen Bürgern gegenüber. Tatsächlich wird die Einhaltung eines EU-grundrechtskonformen Schutzniveaus auch weiterhin alleine in das Ermessen der USA gestellt. Dies ist eine Kapitulation in Sachen Datenschutz und IT-Sicherheit. Die EU-Kommission scheut die Konsequenzen der derzeit gebotenen Einstufung der USA als unsicheres Drittland und verkennt, dass die europäischen, insbesondere auch deutschen Unternehmen wirtschaftlich von einem konsequenten Handeln hätten profitieren können. Stattdessen präsentiert die Kommission einen Schnellschuss, der sich auf die Beteuerungen eines Verhandlungspartners verlässt, wegen dessen verdeckten Datenzugriffs das Vorgänger-Abkommen ("Safe Harbor") gescheitert war. Für Unternehmen, die Daten in die USA übermitteln, stellt sich die Frage, ob dies auf einer derart unsicheren Grundlage erfolgen kann.

24. Der IT-Planungsrat, das zentrale Gremium für die föderale Zusammenarbeit in der Informationstechnik, hat neue "Ergänzende Vertragsbedingungen" (EVB-IT) für die Beschaffung von Hardware beschlossen. Kernelement der neuen EVB-IT ist eine verpflichtende "No backdoors"-Klausel. TeleTrusT begrüßt diese Präzisierung ausdrücklich. Gemäß den neuen EVB-IT müssen IT-Dienstleister gewährleisten, dass die von ihnen zu liefernde Hardware frei von Funktionen ist, die die Integrität, Vertraulichkeit und Verfügbarkeit der

Hardware, anderer Hard- und/oder Software oder von Daten gefährden und dadurch den Vertraulichkeits- oder Sicherheitsinteressen des Auftraggebers zuwiderlaufen. Die neuen Klauseln sind ein Beitrag zur digitalen Souveränität, denn Implementierung von verdeckten Zugangsmöglichkeiten schwächt das Vertrauen in IT-Sicherheitslösungen und erhöht das Risiko eines Schadens. Insbesondere IT-Sicherheitsprodukte 'made in Germany' müssen sich auch weiterhin durch besondere Vertrauenswürdigkeit auszeichnen, um in Zukunft den Digitalisierungsprozess verlässlich umsetzen zu können. Die TeleTrusT-Initiative "IT Security made in Germany" (ITSMIG) und das darauf basierende Qualitätszeichen spiegeln diesen Vertrauenswürdigkeitsanspruch wider.

25. Unsichere IT stellt einen Sachmangel und Schlechtleistung dar. Es bedarf einer konsequenten Anwendung von Sanktionen und Haftungsregelungen bei unsicherer IT. Moderne, zuverlässige IT-Sicherheitsmechanismen sind erforderlich. Wer andere gefährdet, indem er schlecht gesicherte Geräte herstellt oder in Umlauf bringt, der muss dafür zur Verantwortung gezogen werden. Verantwortungsübernahme schließt sowohl Ersatz von nachgewiesenem Schaden als auch Bußgelder ein. Dies hätte überdies zur Folge, dass Unternehmen und Telekommunikationsanbieter verstärkt Zertifizierungen von den Herstellern verlangten, um sich selbst abzusichern. Der Sicherheitsstandard bei vernetzten Geräten und den damit betriebenen privaten oder öffentlichen Infrastrukturen würde dadurch steigen. Notwendig sind proaktive Mechanismen, die Angriffe grundsätzlich verhindern. Zu erreichen ist

das beispielsweise durch die insbesondere von deutschen Anbietern favorisierte verstärkte Virtualisierung, Separierung und Datenflusskontrolle in IT-Systemen.

26. Die sog. Blockchain ist eine Chance für die IT-Sicherheitsindustrie. Die kryptografische Währung Bitcoin und die als Blockchain bekannte dahinterstehende Technologie sind aktuelle Hype-Themen, jedoch inhaltlich einem breiteren Publikum noch weitgehend unbekannt. Grundlegend ist, dass Blockchains kryptographische Funktionen verwenden und als dezentrale Systeme arbeiten. Sichere IT spielt dabei eine wesentliche Rolle. Schließlich geht es darum, mit der Blockchain-Technologie vertrauenswürdige IT- und Netz-Infrastrukturen zu entwickeln. Die praktische Nutzung in Verbindung mit IT-Sicherheit ist daher zentrales Thema. Dabei können am Ende sowohl komplett offene Anwendungsfälle als auch Anwendungen für geschlossene Nutzergruppen in Betracht kommen, exemplarisch im Umfeld von elektronischen Identitäten und Zugriffskontrollmechanismen. Für TeleTrusT ist in Bezug auf die Blockchain insbesondere 'IT Security made in Germany' von Bedeutung. Deutschland kann den Ausbau einer sicheren IT-Infrastruktur vorantreiben und nationale und internationale Vertrauensräume mit sicheren IT-Anwendungen schaffen. Das enorme Potential der Blockchain-Technologie bietet hierfür interessante Möglichkeiten.

27. Das von TeleTrusT und dem IT-Anwenderverband VOICE erstellte und an die Politik adressierte Leitliniendokument "Manifest für IT-Sicherheit" stellt Defizite und Probleme im IT-Security-Umfeld dar, die dringend behoben werden müssen. Ausgangspunkt ist die Erkenntnis, dass der Grad an IT-Sicherheit und Vertrauenswürdigkeit in Deutschland zur Zeit nicht ausreichend ist. Es gibt keine Perimeter und es fehlt allgemein an Wissen, Verständnis, Einschätzungskompetenz, Technologien und Vorgehensweisen. Viele IT-Produkte erreichen nicht den nötigen Reifegrad hinsichtlich IT-Sicherheit, um ein grundlegendes Maß an Vertrauenswürdigkeit zu etablieren. TeleTrusT und VOICE haben gemeinsam sechs Thesen erarbeitet:

1. Ohne IT-Sicherheit gelingt keine nachhaltige Digitalisierung.
2. Gemeinsam wirkungsvollere IT-Sicherheitslösungen nutzen.
3. Verschlüsselung und Vertrauen sind die digitalen Werkzeuge für informationelle Selbstbestimmung.
4. Security-by-Design, Privacy-by-Design und nachvollziehbare Qualitätssicherung sind unabdingbar.
5. Wir benötigen eigene Souveränität über unsere IT-Sicherheitsinfrastrukturen.
6. Cyber War, Cyber-Sabotage und Cyber-Spionage werden immer bedrohlicher.

Die in dem Manifest formulierten Ziele und Absichten ergänzen die im November 2016 von der Bundesregierung beschlossene "Cyber-Sicherheitsstrategie für Deutschland". Vertrauensvolle Zusammenarbeit und enger Austausch zwischen Staat und Wirtschaft sind unabdingbar, um die Cyber-Sicherheit in Deutschland dauerhaft auf hohem Niveau zu gewährleisten.

28. Der Gesetzgeber hat mit dem "Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens" die Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung und die Online-Durchsuchung erweitert und Grundrechte in Bezug auf das Fernmeldegeheimnis eingeschränkt. TeleTrusT wendet sich gegen diese legalisierte Schwächung von modernen IT-Systemen. Die vom Gesetzgeber legalisierten Maßnahmen führen dazu, das Vertrauen in moderne IT-Systeme im Allgemeinen und in die angebotenen vertrauenswürdigen Lösungen zu erschüttern. Sie sind damit industriepolitisch kontraproduktiv und schädigend für den weiteren notwendigen Digitalisierungsprozess. Die geschaffenen Möglichkeiten stehen im Widerspruch zur politischen Zielsetzung, "Deutschland zum Verschlüsselungsstandort Nr. 1" zu entwickeln. Die Eignung zur Verbrechensaufklärung ist fragwürdig, weil Straftäter beispielsweise auf andere Kommunikationsmöglichkeiten ausweichen werden. Die Beeinträchtigung des Grundvertrauens der Öffentlichkeit in den Schutz der kommunikativen Privatsphäre steht in keinem vernünftigen Verhältnis zur möglichen Ausbeute bei Strafverfolgungsmaßnahmen.

29. Die Europäische Kommission hat einen Regulierungsvorschlag veröffentlicht, der auch einen künftigen Europäischen Zertifizierungs- und Kennzeichnungsrahmen für IKT-Sicherheit betrifft. Er soll die Sicherheitseigenschaften von Produkten, Systemen und Diensten, die bereits in der Entwurfsphase ("security by design") integriert sind, verbessern. Die gute Absicht ist erkennbar, zumal ein erhöhter Schutz der Bürger und Unternehmen durch bessere Cybersicherheits-Vorkehrungen erstrebenswert ist. Dennoch hat der Vorschlag erhebliche fachliche Mängel. Darüber hinaus fehlt es an Offenheit und Transparenz, wie man sie von Normensetzung erwarten kann, die der Unterstützung der EU-Gesetzgebung dienen soll.

Der Vorschlag wird als notwendiger und grundlegender Beitrag zur Cyber-Sicherheit in digitalen Infrastrukturen angesehen. Die Entwicklung und der Einsatz der neuen Digitaltechnologien mit ihren erhöhten inhärenten Risiken bedürfen eines nachhaltigen Rahmenplans, der einschlägige technische Normen und Zertifizierungsdienste im "Digitalen Binnenmarkt" bereitstellt. Dies führt zu sicheren Produkten, Systemen und Diensten bereits vor Markteintritt und während ihres gesamten Lebenszyklus. Der Vorschlag orientiert auf umfassende Befugnisse für die EU-Kommission, zu entscheiden, welche Cybersicherheits-Schemata innerhalb der EU erforderlich sind, welche Normen für ein Schema gelten und welche Produkt- oder Dienstetypen erfasst werden. Ein Schema kann Smart Meters, IoT-tragbare Geräte, Datenbanken, Cloud-Dienste, Smartphones etc. umfassen, in der Tat also jedes IKT-Produkt. Sollten keine anwendbaren Normen für ein Schema vorhanden sein, werden die Anforderungen, die zur Zertifizierung eines Schemas erfüllt werden müssen, ohne Konsultation in das Schema integriert.

Der EU-Agentur für Network and Information Security (ENISA) wird das Vorschlagsrecht für Schemata zugeschrieben, aber die endgültige Entscheidung, wann ein neues EU-Schema erforderlich ist und welche Produkte und Dienste erfasst werden, bleibt ausschließlich in der Hand der EU-Kommission. Es gibt keine Beteiligung der Mitgliedstaaten, des Europäischen Rates, des Europäischen Parlaments, nationaler Normenorganisationen, gesellschaftlicher Interessengruppen oder der Industrie. Dass ein Schema zunächst freiwillig anzuwenden ist, ist ein schwaches Argument zur Verteidigung einer Verordnung, die der EU-Kommission zu viel Macht verleiht.

Der neue Rahmenplan kann nur unter folgenden Voraussetzungen gelingen:

1. Der Rahmenplan migriert vorhandene Zertifizierungsinfrastrukturen ohne Betriebsunterbrechung, besonders SOGIS-MRA ("Senior Officials Group Information Systems Security - Mutual Recognition Arrangement", aktuell mit 14 Mitgliedstaaten, kompetenten Schemata und privaten Prüfstellen; initiiert Anfang der neunziger Jahre durch die EU-Kommission, große Industrieanerkennung und Weltmarktposition).
2. Zertifizierung muss auf offene Normen setzen, die Wettbewerb zwischen Prüfstellen bzw. Schemata sowie zwischen den geeignetsten Sicherheitslösungen für ein festgelegtes Sicherheitsproblem ermöglichen.
3. Der Rahmenplan kann Ergebnisse analog zum rasanten Tempo technologischer Änderungen erzielen und die Marktbedürfnisse rechtzeitig und wirtschaftlich befriedigen.
4. Eine leistungsstarke Beziehung zwischen dem Rahmenplan und den Europäischen Normungsorganisationen (ESO) kann aufgebaut werden.

5. Was die IKT-Sicherheitsaspekte betrifft, werden die Richtlinien und Verordnungen der EU-Kommission für jeden vertikalen Digitalmarkt die Anforderungen an geeignete technische Sicherheitsnormen und Zertifizierungen prüfen und das Certification Board entsprechend regelmäßig einbeziehen. Falls ein Vertikalsektor nicht harmonisiert werden kann, wird die Vereinheitlichung der technischen Normen und Zertifizierungen schwer erreichbar sein. IT-Sicherheit betrifft auch Netzwerksicherheit, die öffentliche bzw. nationale Sicherheit sowie die digitale Souveränität. IT-Sicherheit ist nicht nur Anliegen des Digitalbinnenmarktes, sondern auch der Mitgliedsstaaten. Das gilt insbesondere für Kryptonormen und die Qualifikation der Prüfstellen.

Deshalb muss ein künftiges Europäisches IKT-Zertifizierungs- und Kennzeichnungsrahmenwerk

- ein "European Cyber Security Certification Board" etablieren, besetzt mit Vertretern der Mitgliedsstaaten in Abstimmung mit den ESO und dem European Data Protection Board (EDPB), mit der Verantwortung, seine Themenbereiche sowie Arbeitsgruppen aufzubauen,
- die Generaldirektionen der EU-Kommission bei der Entwicklung der Kommunikationen, Richtlinien und Verordnungen für Vertikalsektoren unterstützen, so dass Standardisierung und Zertifizierung in einer sehr frühen Phase vorbereitet werden und Synergien zwischen den vertikalen Digitalisierungssektoren erzeugt werden können,
- SOGIS-MRA von einer Aktivität einzelner Mitgliedsstaaten in eine gesamteuropäische Aktivität migrieren,

- die Unabhängigkeit der Standardisierung und Auswertung gewährleisten, indem ein geeignetes Akkreditierungssystem für Prüfstellen bereitgestellt wird und die Akkreditierungsverordnung mit Hilfe einer zusätzlichen sektorspezifischen Ausnahmeregelung gemäß Erwägungsgrund Nr. 5 in 765/2008 verbessern,
- eine Rolle für die ENISA etablieren, um die Sekretariats- und organisatorische Infrastruktur für das (neue) European Cyber Security Certification Board bereitzustellen,
- Mitgliedsstaaten und Industrie unterstützen, um Innovationen für bessere IT-Sicherheit einzuleiten und Wettbewerbsgleichheit für die europäische Industrie im Weltmarkt zu schaffen.

30. Die in TeleTrusT organisierte IT-Sicherheitsbranche und Wirtschaftsverbände fordern die regierungsbildenden Parteien auf, ein jährliches Budget von mindestens 1 Milliarde Euro für die Stärkung der Cybersicherheit von Behörden und Wirtschaft aufzustellen. Mit dem Geld sollen dringend erforderliche finanzielle und organisatorische Maßnahmen ermöglicht werden, die das Cybersicherheitsniveau in Unternehmen und Behörden deutlich erhöhen. Der Verband begründet seine Forderungen mit der zunehmenden Digitalisierung in allen Branchen und der gleichzeitig unzureichenden Ausstattung von Behörden und Wirtschaft hinsichtlich der Absicherung ihrer IT-Systeme.
Die digitale Agenda der bisherigen Bundesregierung hat zwar die politischen Handlungsstränge für die digitale Transformation formuliert. Konkrete Ziele und Umsetzungspläne bezüglich Cybersicherheitsstrategien von Behörden

und Wirtschaft sind jedoch nicht in Sicht. Für eine deutliche Erhöhung des Cybersicherheitsniveaus sind daher konkrete Schritte und Maßnahmen erforderlich, die über Regulierungen hinausgehen. Mit der geforderten Investition von 1 Milliarde Euro jährlich würde der digitale Standort Deutschland nachhaltig attraktiver werden - auch für ausländische Investoren. Denn Investitionen in Cybersicherheit wirken flächendeckend auf die Verfügbarkeit aller digital vernetzten Infrastrukturen. Gleichzeitig würde die neue Bundesregierung die Chance nutzen, die eigene IT-Sicherheitswirtschaft zu stärken und europäische und internationale Kooperationsprojekte aufzubauen. TeleTrusT fordert daher folgende Maßnahmen:

- Personelle Stärkung des Bundesamtes für Sicherheit in der Informationstechnik" (BSI) - Zulassungs- und Zertifizierungsverfahren müssen beschleunigt werden, um so nachweislich sichere digitale Prozesse, Produkte und Lösungen schneller den Anwendern zur Verfügung stellen zu können. Auch Beratung und Unterstützung von Behörden und Wirtschaft müssen ausgebaut werden, damit diese sich im Vorfeld oder bei akuten Angriffen besser schützen können.
- Neue Anreizsysteme, mit denen Behörden und Unternehmen die vom BSI empfohlenen, dem Stand der Technik entsprechenden IT-Sicherheitsmaßnahmen aufbauen können
- Erhöhung des BSI-Budgets für die Entwicklung neuer gesamtwirtschaftlicher und staatlich erforderlicher Basis-Sicherheitsprodukte
- Etablierung breiter Programme für Wirtschaft und Behörden, um die vorhandenen Cybersicherheits-Lösungen der deutschen IT-Sicherheitswirtschaft besser bekannt zu machen
- Investitionen in Kooperationsprogramme zwischen Anwendern und Industrie

- Bei der Erarbeitung von innovativen Lösungen, Maßnahmen und Produkten rund um die Cybersicherheit sollten verstärkt Synergien zwischen Anwendern und IT-Sicherheitsindustrie genutzt werden. Usability- und Betriebsanforderungen großer IT-Architekturen müssen zudem an den Bedürfnissen des Mittelstandes ausgerichtet werden.

TeleTrusT-Positionen zu speziellen Themen:
https://www.teletrust.de/publikationen/stellungnahmen/

TeleTrusT-Konzept "IT-Sicherheitsstrategie für Deutschland":
https://www.teletrust.de/it-sicherheitsstrategie/

TeleTrusT/VOICE - "Manifest IT-Sicherheit":
https://www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/

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.

Kontakt:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 310
Fax: +49 30 400 54 311
https://www.teletrust.de

TeleTrusT
Pioneers in IT security.


TeleTrusT
Pioneers in IT security.