

## ***TeleTrust-Positionen***

## **Impressum**

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

Herstellung:

DATEV eG, Nürnberg

© 2017 TeleTrusT

## ***Zentrale TeleTrust-Positionen***

TeleTrust begrüßt zentrale Festlegungen zu "IT-Sicherheit" im aktuellen CDU/CSU/SPD-Koalitionsvertrag. Die jetzige Legislaturperiode bietet die Chance, verlorenes Terrain in der IT-Sicherheitstechnologie wiederzugewinnen und Deutschland im internationalen Kontext wegweisend aufzustellen. TeleTrust befürwortet insbesondere die Punkte:

- Ausbau der Internet-Infrastruktur Deutschlands und Europas als Vertrauensraum;
- Eintreten für eine europäische Cybersicherheitsstrategie;
- Maßnahmen zur Rückgewinnung technologischer Souveränität;
- Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur einschließlich Entwicklung sicherer Soft- und Hardware und sicherer Cloud-Technologie;
- Schaffung eines IT-Sicherheitsgesetzes mit verbindlichen Mindestanforderungen für kritische Infrastrukturen;
- Pflicht, "erhebliche IT-Sicherheitsvorfälle" zu melden;
- Verpflichtung der Bundesbehörden, 10 % ihres IT-Budgets für Systemicherheit zu verwenden;
- Weiterentwicklung und Verbreitung von sicheren Kartenlesegeräten und Kryptographielösungen;
- Initiierung eines Spitzenclusters "IT-Sicherheit und kritische IT-Infrastruktur";
- Einführung einer Haftung von IT-Herstellern und Diensteanbietern für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte.

## ***TeleTrust-Leitpositionen***

1. Insbesondere vertrauenswürdiger, 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 Gruppensertifikate 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 Schlüssel hinterlegung 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-Verhandlungsträger:

- 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.



TeleTrusT-Positionen zu speziellen Themen:

<https://www.teletrust.de/publikationen/stellungnahmen/>

TeleTrusT-Konzept "IT-Sicherheitsstrategie für Deutschland":

<https://www.teletrust.de/it-sicherheitsstrategie/>

## **TeleTrust - Bundesverband IT-Sicherheit e.V.**

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 Mitgliedschaft 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:**

TeleTrust - Bundesverband IT-Sicherheit e.V.

Dr. Holger Mühlbauer

Geschäftsführer

Chausseestraße 17

10115 Berlin

Tel.: +49 30 400 54 310

Fax: +49 30 400 54 311

<https://www.teletrust.de>



