TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Jahresbericht 2017

SecurITy made in Germany
Trust Seal
www.teletrust.de/itsmig

T.I.S.P.
TeleTrusT Information Security Professional

T.P.S.S.E.
TeleTrusT Professional for Secure Software Engineering

TeleTrusT EBCA
European Bridge Certificate Authority

Impressum

Herausgeber:

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

Abbildungen: TeleTrusT

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 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.

www.teletrust.de

TeleTrusT - Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin

Telefon: +49 30 4005 4310

E-Mail: info@teletrust.de

Inhaltsverzeichnis

Vorstand und Geschäftsstelle 2017

► TeleTrusT-Vorstand

Prof. Dr. Norbert Pohlmann

Direktor des if(is) Institut für Internet-Sicherheit, Westfälische Hochschule, Gelsenkirchen

Vorsitzender des TeleTrusT-Vorstands

Dr. Rainer Baumgart

Vorstandsvorsitzender der secunet security AG, Essen

Stellvertretender
Vorsitzender des TeleTrusT-Vorstands

Ammar Alkassar

Geschäftsführer der Rohde & Schwarz Cybersecurity GmbH

Mitglied des TeleTrusT-Vorstands

RA Karsten U. Bartels, LL.M.

Partner bei HK2 Rechtsanwälte, Berlin

Mitglied des TeleTrusT-Vorstands

► TeleTrusT-Geschäftsführer

Dr. Holger Mühlbauer

Geschäftsführer

Telefon: +49 30 400 54 306
Telefax: +49 30 400 54 311
E-Mail: holger.muehlbauer@teletrust.de

► TeleTrusT-Geschäftsstelle

Martin Fuhrmann

Projektkoordinator

Telefon: +49 30 400 54 305
Telefax: +49 30 400 54 311
E-Mail: martin.fuhrmann@teletrust.de

Marieke Petersohn

Projektkoordinatorin

Telefon: +49 30 400 54 308
Telefax: +49 30 400 54 311

Nicolai Guthmann

Projektkoordinator

Telefon: +49 30 400 54 308
Telefax: +49 30 400 54 311
E-Mail: nicolai.guthmann@teletrust.de

Marion Gutsell

Assistentin

Telefon: +49 30 400 54 310
Telefax: +49 30 400 54 311

Vi Linh Tran-Graef

Assistentin

Telefon: +49 30 400 54 307
Telefax: +49 30 400 54 311
E-Mail: vilinh.tran-graef@teletrust.de

Ida Köhler

Projektassistentin

Telefon: +49 30 400 54 309
Telefax: +49 30 400 54 311

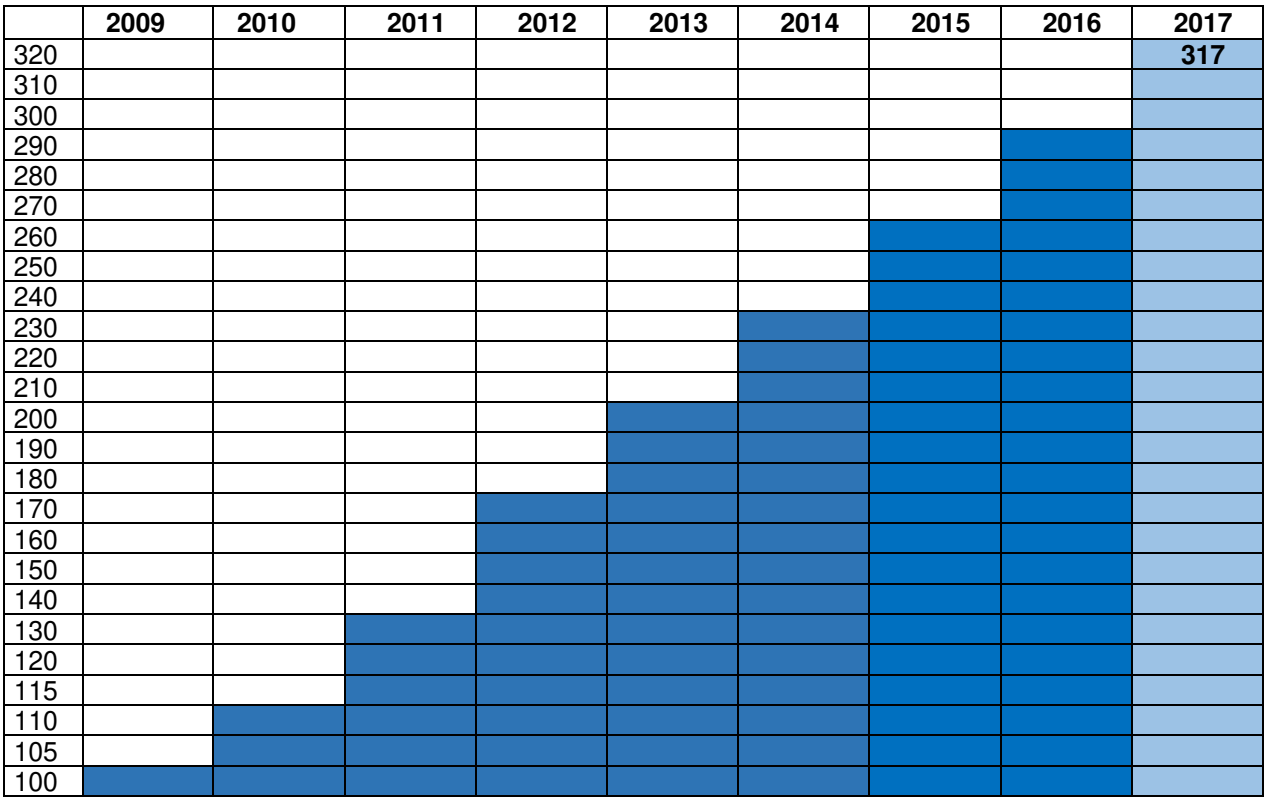
Helke Brauch

Projektassistentin

Telefon: +49 30 400 54 309
Telefax: +49 30 400 54 311
E-Mail: helke.brauch@teletrust.de

Verbandsentwicklung 2017

► **Mitgliederzahl**



► **TeleTrusT-Arbeitsgruppen und -Lenkungsgremien 2017**

TeleTrusT-Arbeitsgruppen:

"Biometrie"	Leitung: Prof. Dr. Christoph Busch, Fraunhofer IGD Alexander Nouak, Fraunhofer IGD Georg Hasse, secunet
"Cloud Computing"	Leitung: Oliver Dehning, Hornetsecurity
- AK "Verschlüsselung"	Leitung: Peter Hansemann, ICN
"EBCA/Technik"	Leitung: Hendrik Koy, Deutsche Bank
"Forum elektronische Vertrauensdienste"	Leitung: Christian Seegebarth, Bundesdruckerei Clemens Wanko, TÜViT
"Gesundheitstelematik"	Leitung: Dr. Christoph-F. Goetz, KV Bayern
"Informationssicherheitsmanagement"	Leitung: Werner Wüpper, WMC
"IT Security made in Germany"	Leitung: NEU: Peter Rost, Rohde + Schwarz Cybersecurity
"IT-Sicherheit in der Marktforschung"	Leitung: Erich Wiegand, ADM bzw. NEU Bettina Klumpe, ADM
"Mobile Security"	Leitung: Ronny Kaminski, Sama Partners
"Recht"	Leitung: RA Karsten U. Bartels, HK2 RA Dr. Axel Frhr. v.d. Bussche, Taylor Wessing
- AK "Stand der Technik"	Leitung: Tomasz Lawicki, Schwerhoff
"RSA"	Leitung: Prof. Dr. Helmut Reimer
"SICCT"	Leitung: Jürgen Atrott, TÜViT
"Smart Grids / Industrial Security"	Leitung: Steffen Heyde, secunet
"Blockchain"	Leitung: Dr. André Kudra, esatus
"Politik"	Leitung: Oliver Dehning, Hornetsecurity
NEU: "ECSO" (Koordinierungskreis)	Leitung: Gerd Müller, secunet

TeleTrusT-Lenkungsgremien:

Vorstand	Vorsitzender: Prof. Dr. Norbert Pohlmann, if(is) Stellv. Vorsitzender: Dr. Rainer Baumgart, secunet
"EBCA"	Sprecher: Markus Wichmann, Siemens
"T.I.S.P."	Sprecher: Christoph Weinman, Secorvo bzw. NEU Birgitte Baardseth, is-its
"T.P.S.S.E"	Sprecherin: Petra Barzin, Secorvo

► TeleTrusT-Regionalstellen 2017

"Bremen" (repräsentiert durch Otaris)
"Chemnitz" (repräsentiert durch Digitronic)
"Dresden" (repräsentiert durch T-Systems MMS)
"Düsseldorf" (repräsentiert durch Exceet)
"Frankfurt/M." (repräsentiert durch QGroup)
NEU "Hagenberg" - AT - (repräsentiert durch FH Hagenberg OÖ)
"Hamburg" (repräsentiert durch Wüpper Management Consulting)
"Kiel" (repräsentiert durch 8ack)
"Köln" (repräsentiert durch FSP)
"Leipzig" (repräsentiert durch Rohde & Schwarz)
NEU: "Mannheim" (repräsentiert durch Sama Partners)
"München" (repräsentiert durch itWatch)
"Silicon Valley" - US -
"Stuttgart" (repräsentiert durch CenterTools bzw. NEU Detack)
"Wien" - AT - (repräsentiert durch AIT)

► Durch TeleTrusT wahrgenommene Beirats- und Komiteemitgliedschaften (Auswahl):

BMWi: Beirat Exportinitiative IT-Sicherheitswirtschaft
BMWi: IT-Standardisierungsbeirat
BMWI: TaskForce IT-Sicherheit in der Wirtschaft
BSI-Kongress: Programmkomitee
D-A-CH Security: Programmkomitee
DsiN - Deutschland sicher im Netz e.V.: Beirat
DIN: Beirat Koordinierungsstelle IT-Sicherheitsnormung
DTCE - Digital Trust and Compliance Europe: Board of Directors
ECSO - European Cybersecurity Organisation: Board of Directors
it-sa: Ausstellerbeirat
it-sa Brasil: Messebeirat
NEU: it-sa India: Messebeirat
OmniSecure: Programmkomitee
RSA Conference: Exhibitor Advisory Council

► TeleTrusT-Verbandsbeziehungen 2017

Assoziierte Mitgliedschaften

Deutschland:
ASW-M - Allianz für Sicherheit in der Wirtschaft Mitteldeutschland e.V.
AWV - Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V.
BVSW - Bayerischer Verband für Sicherheit in der Wirtschaft e.V.
BISG - Bundesfachverband der IT-Sachverständigen und -Gutachter e.V.
CAST e.V. - Competence Center for Applied Security Technology
DAV IT - Arbeitsgemeinschaft Informationstechnologie im Deutschen Anwaltverein e.V.
DGOF - Deutsche Gesellschaft für Online-Forschung e.V.
DVPT - Deutscher Verband für Post, Informationstechnologie und Telekommunikation e.V.

eco - Verband der Internetwirtschaft e.V.
eurobits e.V.
EuroCloud Deutschland_eco e.V.
GDD - Gesellschaft für Datenschutz und Datensicherung e.V.
networker NRW e.V.
NIFIS - Nationale Initiative für Informations- und Internet-Sicherheit e.V.
OAV - German Asia-Pacific Business Association
SIBB - Verband der IT- und Internetwirtschaft in Berlin und Brandenburg e.V.
SILICON TRUST
VeR - Verband elektronische Rechnung e.V.
VfS - Verband für Sicherheitstechnik e.V.
VOI - Verband Organisations- und Informationssysteme e.V.

Belgien:
LSEC - Leaders in Security

Finnland:
FISC - Finnish Information Security Cluster

Frankreich:
FNTC - Fédération Nationale des Tiers de Confiance
NEU: Hexatrust

Großbritannien:
EEMA - European Association for e-Identity and Security

Österreich:
AUSTRIAPRO - Verein zur Förderung der elektronischen DÜ im Geschäftsverkehr (WKO)
NEU: KSÖ - Kuratorium Sicheres Österreich

Schweiz:
ISSS - Information Security Society Switzerland
Swiss Cyber Storm

USA:
ESRA - Electronic Signature and Records Association
FIDO - The FIDO Alliance
GABA California - German American Business Association California
GCRI - German Center for Research and Innovation - New York
Smart Card Alliance

► Weitere reguläre Mitglieds- und Partnerorganisationen von TeleTrusT

ADM - Arbeitskreis Deutscher Markt- und Sozialforschungsinstitute e.V.
AV - Afrika-Verein der deutschen Wirtschaft e.V.
Bankenverband - Bundesverband deutscher Banken e.V.
BDK - Bund Deutscher Kriminalbeamter e.V.
bevh - Bundesverband E-Commerce und Versandhandel Deutschland e.V.
BITMi - Bundesverband IT-Mittelstand e.V.
BNotK - Bundesnotarkammer K.d.ö.R.
BvD - Berufsverband der Datenschutzbeauftragten e.V.
BVK - Bundesverband Deutscher Kapitalbeteiligungsgesellschaften e.V.
DFN - Deutsches Forschungsnetz e.V.
DsiN - Deutschland sicher im Netz e.V.
EAB - European Association for Biometrics
EICAR - European Institute for Computer Anti-Virus Research
GA - German Accelerator
KBV - Kassenärztliche Bundesvereinigung, K.d.ö.R.
KVB - Kassenärztliche Vereinigung Bayerns, K.d.ö.R.

nrw.uniTS
SIGNATURE - European Security Innovation Network
NEU: WPIA - World Privacy and Identity Association

► Sonstige TeleTrusT-Mitgliedschaften und Verbindungen

BCTT - Business Coalition for Transatlantic Trade (USA)
CEN-CENELEC-ETSI Cyber Security Consultative Group (Europa)
DGAP - Deutsche Gesellschaft für Auswärtige Politik e.V. (Deutschland)
DGVM - Deutsche Gesellschaft für Verbandsmanagement e.V. (Deutschland)
DIN - Deutsches Institut für Normung e.V. (Deutschland)
DTCE - Digital Trust and Compliance Europe (Europa)
ECSO - European Cyber Security Organisation (Europa)
ENX Association (Europa)
ETSI - European Telecommunications Standards Institute (Europa)
GKV - Spitzenverband (Spitzenverband Bund der Krankenkassen; Deutschland)
Verbraucher sicher online (Deutschland)

► TeleTrusT in der Normung und Standardisierung

BMWi
TeleTrusT ist Mitglied des Beirates für Standardisierung in der Informations- und Kommunikationstechnologie (BSIKT) im Bundeswirtschaftsministerium sowie des "Beraterkreises Normung" im BMWi, in dem u.a. die "Deutsche Normungsstrategie" bzw. die Rolle der Normung aus Ressort-, Wirtschafts- und Verbändesicht erörtert und mitgestaltet wird.

DIN
TeleTrusT ist reguläres Mitglied des Deutschen Instituts für Normung (DIN). TeleTrusT ist aktives Mitglied der DIN-Koordinierungsstelle IT-Sicherheitsnormung (KITS), des DIN-Projektbeirates "Sichere Digitale Identitäten" und von DIN benanntes aktives Mitglied der CEN/CENELEC Cybersecurity Standardisation Coordination Group. TeleTrusT unterstützt die jährliche "KITS-Konferenz" des DIN sowie anlassbezogen Veranstaltungen der DIN-Akademie und des Beuth-Verlages.

Austrian Standards
TeleTrusT ist Mitglied in mehreren Komitees von Austrian Standards International, dem österreichischen Normungsinstitut, insbesondere im ONK 260 (Normung und Standardisierung von IT-gestützter Markt-, Meinungs- und Sozialforschung; ISO/TC 225).

CEN/CENELEC
TeleTrusT begleitet die Normungs- und Standardisierungsaktivitäten bei CEN bzw. CENELEC und ist über das DIN benanntes Mitglied der Advisory Group für CEN-CLC/JTC 13 "Cybersecurity and Data Protection".

ETSI
TeleTrusT ist reguläres Mitglied im European Telecommunications Standards Institute (ETSI), hat Stimmrecht in der ETSI-Generalversammlung und beteiligt sich mit Expertenbenennungen an ETSI-Projekten, beispielsweise im Themenbereich Elektronische Signaturen ("PAdES"). TeleTrusT unterstützt anlassbezogen ausgewählte ETSI-Veranstaltungen, zum Beispiel zum Thema "Quantum Cryptography". Ausgewählte ETSI-Rundrufe nach Expertennominierungen werden unter den TeleTrusT-Mitgliedern zirkuliert, ebenso Beteiligungsaufrufe für Testläufe (eSignature Plugtests).

ISO
Neben dem Engagement zahlreicher TeleTrusT-Mitglieder in ISO-Aktivitäten (ISO/IEC/JTC 1), zum Beispiel auf dem Gebiet biometrischer Anwendungen, ist TeleTrusT als Verband in ISO/TC 225 vertreten, in dem an Normen zu IT-gestützter Markt-, Meinungs- und Sozialforschung gearbeitet wird.

1 Politik

► TeleTrusT und VOICE überreichen "Manifest zur IT-Sicherheit" an BMI und BMWi

Notwendige Ergänzung der "Cyber-Sicherheitsstrategie für Deutschland"

Gemeinsames Thesenpapier von TeleTrusT und Bundesverband der IT-Anwender (VOICE) weist auf Defizite der IT-Sicherheit und bietet Handlungsempfehlungen

Zum Auftakt der CeBIT 2017 übergaben Vertreter von TeleTrusT und VOICE das gemeinsam erarbeitete "Manifest zur IT-Sicherheit" an die Bundesregierung. BMI-Staatssekretär Klaus Vitt, IT-Beauftragter der Bundesregierung, und Andreas Könen, Leiter der Stabsstelle "IT- und Cybersicherheit, sichere IT" im BMI, nahmen das Dokument im Beisein von BSI-Präsident Arne Schönbohm entgegen. Das von TeleTrusT- und VOICE-Experten ausgearbeitete und an die Politik adressierte Leitliniendokument "Manifest für IT-Sicherheit" stellt Defizite und Probleme im IT-Security-Umfeld dar, die dringend behoben werden müssen. Das Manifest zeigt, dass Unternehmen die Digitalisierung ernst nehmen und sich für sichere Lösungen einsetzen. 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 und VOICE haben gemeinsam sechs Thesen erarbeitet, die jeweils spezifische "Gemeinsame Aufgaben" innerhalb jeder These skizzieren, wie vorhandene Herausforderungen erfolgreich bewältigt werden können:

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.

Zugleich wird aufgezeigt, wie sich Defizite beheben lassen und eine angemessene Risikovorsorge in der IT erreicht werden kann. 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.

Manifest-Mitherausgeber und TeleTrusT-Vorsitzender Prof. Dr. Norbert Pohlmann erkennt einen starken Hebel bei den Anwendern, mit dem sich mehr IT-Sicherheit erreichen lässt: "Wir müssen vom angebotsgetriebenen zum anforderungsgetriebenen IT-Sicherheitsmarkt gelangen. Dazu sollten die Anwenderunternehmen gemeinsam ihre Einkaufsmacht fair nutzen. Eine enge Zusammenarbeit zwischen den Herstellern und Anwendern ist nötig, um angemessene, wirkungsvolle, sichere und vertrauenswürdige IT-Lösungen in den operativen Einsatz zu bringen und umfangreiche und übergreifende IT-Konzepte erfolgreich umzusetzen." Dr. Thomas Endres, Vorsitzender des VOICE-Präsidiums, versteht das Manifest als wichtigen, sichtbaren Zwischenschritt im Dialog zwischen Anwendern, Anbietern, Politik und Wissenschaft.

www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit

► "WannaCry": Weckruf und Warnung

TeleTrusT sieht die weltweit verteilten Angriffe mit der Schadsoftware "WannaCry" als Weckruf für das gemeinsame Handeln der Verantwortlichen in Unternehmen und Organisationen. Gleichzeitig warnt TeleTrusT vor insgeheimer staatlicher Nutzung von IT-Sicherheitslücken.

Bei "WannaCry" handelt es sich offenkundig um Erpressungssoftware, die eine Sicherheitslücke in Microsofts Windows-Betriebssystem ausnutzt. Die US-Geheimdienstbehörde NSA hatte sie für eigene Spähangriffe genutzt und nicht an Microsoft gemeldet. Nun haben Hacker diese Sicherheitslücke, die die

NSA schon lange kennt und nutzt, für einen erfolgreichen Angriff gegen kritische Infrastrukturen, wie z.B. in Deutschland die Deutsche Bahn und Krankenhäuser in Großbritannien, verwendet. Microsoft hatte zwar einen Patch zum Schließen der Lücke veröffentlicht, auf vielen Rechnern wurde die Schwachstelle jedoch nicht rechtzeitig bereinigt.

Prof. Dr. Norbert Pohlmann, TeleTrusT-Vorsitzender: "Dem Ausnutzen von Sicherheitslücken, für die es noch keinen Schutz gibt (Zero Day Exploits), durch staatliche Institutionen erteilen wir eine Absage. Solange Nachrichtendienste erkannte Schwachstellen nicht den betroffenen Herstellern melden, sondern für Zwecke des Ausspähens nutzen, wird der Weg bereitet für Cyberattacken, die eigentlich verhindert werden können."

Besonders beunruhigend ist, dass viele der aktuell betroffenen Systeme zu Betreibern kritischer Infrastrukturen gehören. Gerade dort sollte das Bewusstsein für IT-Sicherheit geschärft sein und entsprechende Vorkehrungen - wie zum Beispiel eine sinnvolle Separierung - getroffen werden, und zwar nicht erst dann, wenn die Betreiber durch Gesetzgebung dazu gezwungen werden.

Dr. Rainer Baumgart, stellvertretender TeleTrusT-Vorsitzender: "Wie viele Weckrufe sind noch erforderlich, damit Unternehmen und Organisationen endlich reagieren und IT-Sicherheit die erforderliche Beachtung schenken? Wieder einmal sind schlecht gewartete, veraltete und ungesicherte, aber dennoch vernetzte Systeme die Ursache für den Erfolg eines großflächigen Angriffs. Das derzeitige IT-Sicherheitsniveau erfüllt die Ansprüche offensichtlich nur ungenügend, obwohl wir insbesondere in Deutschland über vertrauenswürdige IT-Sicherheitstechnologien verfügen."

Es ist höchste Zeit, dass die Verantwortlichen zusammenarbeiten, um mit Hilfe einer gemeinsamen und klaren Cybersicherheitsstrategie dafür zu sorgen, dass der Digitalisierungsprozess nachhaltig sicher und vertrauenswürdig umgesetzt wird, damit solche Angriffe in Zukunft verhindert werden.

Diese essentiellen Forderungen hat ein Gremium aus IT-Sicherheitsexperten bereits in einem "Manifest IT-Sicherheit" ausformuliert. Die aktuelle, schwere Cyberattacke sollte als Initialzündung dienen, um nun Taten folgen zu lassen. Das Manifest ist als Download unter www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/ abrufbar.

► TeleTrusT: Umfrageergebnis der IT-Sicherheitsbranche zur Bundestagswahl 2017

TeleTrusT hat seine Mitglieder, d.h. die organisierte IT-Sicherheitsbranche, durch das Markt- und Meinungsforschungsinstitut SKOPOS befragen lassen, welche IT-sicherheitsrelevanten Themen die Parteien mit Blick auf die Bundestagswahl 2017 adressieren sollten. Das Ergebnis der Befragung, die im Mai 2017 unter reger Beteiligung stattfand, kennzeichnet die Problemlagen der IT-Sicherheit in Deutschland. Zusammengefasst und nach Themen geordnet gibt die IT-Sicherheitsbranche in Deutschland den Parteien diese Merkposten auf:

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 Kryptografie 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.

Weitere Nennungen:
- 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

Siehe auch:

TeleTrusT-Positionen, www.teletrust.de/teletrust-positionen/
IT-Sicherheitsstrategie für Deutschland, www.teletrust.de/it-sicherheitsstrategie/
"Manifest IT-Sicherheit", www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/

► "Bundestrojaner": TeleTrusT-Initiative für Verfassungsbeschwerde

Der Deutsche Bundestag hat per Gesetz Strafermittlern neue technische Möglichkeiten eingeräumt, um verschlüsselte Kommunikation von Verdächtigen in ihren Notebooks und Smartphones mitzulesen und diese unbemerkt durchsuchen zu können ("Gesetz zur effektiveren und praxistauglicheren Ausgestaltung des Strafverfahrens"). Der Gesetzgeber hat damit die Rechtsgrundlagen für die Quellen-Telekommunikationsüberwachung (Quellen-TKÜ) und die Online-Durchsuchung erweitert und Grundrechte in Bezug auf das Fernmeldegeheimnis eingeschränkt. TeleTrusT initiiert eine Verfassungsbeschwerde gegen diese legalisierte Schwächung von modernen IT-Systemen an: Denn anstatt die Bürgerinnen und Bürger aktiv vor IT-Schwachstellen zu schützen, toleriert sie der Staat und hält sie für den potentiellen Einsatz seines "Trojaners" sogar aufrecht.

Mit der gesetzlichen Einsatzerlaubnis für Spionagesoftware ("Bundestrojaner") soll aus staatlicher Sicht der Tatsache Rechnung getragen werden, dass Straftäter über verschlüsselte Messenger-Dienste miteinander kommunizieren. Bei der Quellen-TKÜ werden Nachrichten schon in modernen IT-Systemen, wie Smartphones des Absenders abgefangen, bevor sie verschlüsselt werden. Die Online-Durchsuchung erlaubt es, unbemerkt aus der Ferne das Endgerät eines Verdächtigen nach Hinweisen auf Straftaten zu untersuchen. Für die Zulassung gelten nach dem neuen Gesetz vergleichbar strenge Voraussetzungen wie für die schon jetzt unter Richtervorbehalt erlaubte akustische Wohnraumüberwachung. Im Gesetz ist in allgemeiner Form davon die Rede, dass "mit technischen Mitteln in informationstechnische Systeme eingegriffen wird".

Prof. Norbert Pohlmann, TeleTrusT-Vorsitzender: "Der Staat hat die Pflicht, Bürgerinnen und Bürger zu schützen. Durch die gezielte Offenhaltung und Nutzung von Sicherheitslücken wird diese Schutzpflicht missachtet und das Vertrauen in moderne IT-Systeme staatlich untergraben. Dadurch wird die notwendige Digitalisierung nachhaltig verhindert."

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.

Die beschlossene Gesetzgebung betrifft das verbandspolitische Selbstverständnis von TeleTrusT im Kern. TeleTrusT steht konsequent für Vertrauenswürdigkeit der IT-Systeme und kann nicht tatenlos zusehen, wenn der Gesetzgeber konterkarierende Maßnahmen beschließt, die unsere digitale Zukunft schwächen. TeleTrusT beabsichtigt, nach Konsultation und Beschluss der Mitgliederversammlung eine Verfassungsbeschwerde zu initiieren.

Gleichartige Initiativen haben die Gesellschaft für Freiheitsrechte e.V. (GFF) und der Verein Digitalcourage e.V. angekündigt.

Weiterführende Informationen:

- Stiftung Wissenschaft und Politik (2017-08)
  "Gegenwärtig formiert sich weltweit eine unfreiwillige Allianz von Gegnern der Verschlüsselung. Neben autoritären Regimen setzen auch immer mehr westliche Demokratien darauf, die Kommunikationsverschlüsselung zu schwächen und Spionage-Software auf Smartphones zu nutzen. Damit wird ein globaler Normsetzungsprozess beschleunigt, der die Bemühungen um Cyber-Sicherheit konterkariert. Deutschland sollte sich diesem Trend entgegenstellen und seine Ambitionen als Verschlüsselungsstandort Nummer eins verstärken. Dabei gilt es auch, alternative Ermittlungswege zu finden, damit Terrorverdächtige von Behörden überwacht werden können, ohne dass die Software-Sicherheit der ganzen Bevölkerung leidet."
  www.swp-berlin.org/fileadmin/contents/products/aktuell/2017A56_she.pdf
- Bundestagsarchiv
  "Pro und Contra Staatstrojaner bei der Anhörung zur Strafrechtsreform"
  www.bundestag.de/dokumente/textarchiv/2017/kw22-pa-recht-strafrecht/508168
- Bundestagsarchiv
  "Bundestag gibt Strafermittlern neue Instrumente in die Hand"
  www.bundestag.de/dokumente/textarchiv/2017/kw25-de-aenderung-stgb/511182
- Vorgangsdokumentation auf netzpolitik.org
  netzpolitik.org/2017/wir-veroeffentlichen-den-gesetzentwurf-der-grossen-koalition-zum-massenhaften-einsatz-von-staatstrojanern/
- Bitkom zum sog. "Staatstrojaner" (2017-06)
  www.bitkom.org/Presse/Presseinformation/Bitkom-zum-so-genannten-Staatstrojaner.html

► TeleTrusT-Vergleich: Thema "IT-Sicherheit" in Parteiwahlprogrammen

Vor der Bundestagswahl 2017 hatte TeleTrusT die Wahlprogramme von Parteien ausgewertet und die Aussagen und Positionen zum Themenkreis IT-Sicherheit verglichen. Diese Aussagen werden für eine spätere regelmäßige Überprüfung der tatsächlichen politischen Umsetzung während der neuen Legislaturperiode herangezogen.

Die CDU sieht im Kampf gegen Cyber-Angriffe Investitionsbedarf in Technik und möchte in größerem Umfang entsprechende Fachleute einstellen. Um die digitale Souveränität zu erhalten, möchte auch die SPD Forschung und Ausbildung von Fachkräften sowie Entwicklung von IT-Sicherheitstechnik fördern. Deutschland und Europa sollen zum führenden Standort für IT-Sicherheit und Datenschutz entwickelt sowie das IT-Sicherheitsgesetz fortgeschrieben werden. Die Sozialdemokraten fordern darüber hinaus ein "Völkerrecht des Netzes". Für die FDP muss Verschlüsselungstechnologie gemeinsam mit den Unternehmen weiterentwickelt werden. Die Grünen wollen einen internationalen Verhaltenskodex zur Cybersicherheit etablieren und befürworten öffentliche Förderung von freier Standardsoftware. Durch staatliche Maßnahmen soll nach dem Willen der AfD der Schutz vor Industriespionage erhöht werden.

Die Relevanz des Themas IT-Sicherheit spiegelt sich in den Wahlprogrammen auch bei den Überlegungen zur behördlich-organisatorischen Umgestaltung wieder. Die CDU möchte die Position eines "Staatsministers für Digitalpolitik" im Bundeskanzleramt schaffen, die FDP fordert die Schaffung eines Digitalministeriums. FDP und Grüne möchten das BSI aus dem BMI lösen und unabhängig stellen, die Linke die Unabhängigkeit des BSI stärken und die SPD die Rolle des BSI als neutrale Beratungsinstitution ausbauen. Die AfD spricht sich für einen ganzheitlichen Ansatz einer nationalen Sicherheitsstrategie mit jährlicher Debatte im Bundestag aus und erachtet eine zivil-militärische Zusammenarbeit für notwendig. Die Linke lehnt hingegen Offensivstrategien der Bundeswehr im Cyberraum ab. Bei Aufrechterhaltung staatlicher Eingriffe in informationstechnische Systeme fordern die Piraten weitere Kontrollinstanzen, u.a. ein parlamentarisches Kontrollgremium.

Den "Bundestrojaner" bzw. staatlich verordnete "Backdoors" lehnen Grüne, Piraten und FDP ab. Die Linke ist gegen Online-Durchsuchungen. SPD, Linke und FDP heben die Wichtigkeit von Verschlüsselung hervor. Die Piraten möchten hierfür ein staatlich finanziertes Trustcenter etablieren, das für die Bürger kostenlose Zertifikate zur Verschlüsselung von E-Mails und Dokumenten herausgibt. Piraten und Linke sprechen sich gegen Überwachungssoftware aus, die Piraten fordern darüber hinaus die vollständige Offenlegung des Quellcodes, die Linken ein Exportverbot. Die Piraten setzen sich für die vollständige Abschaffung des sogenannten "Hackerparagraphen" (§ 202c StGB) ein.

Produkt- und Herstellerhaftung bei Schäden durch mangelnde IT-Sicherheit im Sinne von Programmierfehlern oder fehlender bzw. unzureichender Verschlüsselung will die SPD einführen, die FDP zumindest eine Haftung bei Fahrlässigkeit, wenn zum Beispiel nicht der Stand der Technik berücksichtigt wurde. CDU, Grüne, Linke, Piraten und AfD beziehen hierzu keine Stellung.

► Digitalisierung von Wirtschaft und Behörden absichern: IT-Sicherheitsbranche und Wirtschaftsverbände fordern Milliardeninvestitionen

Die in TeleTrusT organisierte IT-Sicherheitsbranche fordert die regierungsbildenden Parteien auf, ein jährliches Budget von mindestens 1 Milliarde Euro für die Stärkung der Cybersicherheit von Behörden und Wirtschaft in den Koalitionsvertrag aufzunehmen. 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.

Die Industrie unterstützt die Forderungen von TeleTrusT. Dr. Klaus Mittelbach, Vorsitzender der Geschäftsführung des Zentralverbands Elektrotechnik- und Elektronikindustrie e.V. (ZVEI): "Cybersicherheit ist ein entscheidender Faktor für die zukünftige internationale Wettbewerbsfähigkeit der deutschen Elektroindustrie. Unsere Lösungen für Industrie 4.0, intelligente Energienetze, digitalisierte Gesundheitswirtschaft, Smart Home und autonomes Fahren werden sich nur dann durchsetzen, wenn sie sowohl innovativ als auch cybersicher sind. Die nächste Bundesregierung muss Cybersicherheit deshalb zu einem Schwerpunkt ihrer Politik machen."

TeleTrusT-Vorsitzender Prof. Norbert Pohlmann ergänzt: "Nachhaltige Digitalisierung kann nur mit umfassender IT-Sicherheit gelingen. Denn gezielte Attacken auf die IT-Systeme können ganze Wirtschaftszweige manipulieren oder gänzlich lahmlegen. Die bisherige Umsetzung der IT-Sicherheitsstrategien ist in Deutschland allerdings unzureichend. Um das Sicherheitsniveau zu erhöhen, sind dringend Investitionen seitens des Bundes notwendig."

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

Zum Vergleich: Großbritannien hat in seiner aktuellen nationalen Cybersicherheitsstrategie beschlossen, in den nächsten fünf Jahren rund zwei Milliarden Euro in Cybersicherheit zu investieren, bei einem Bruttoinlandsprodukt von etwa 2,2 Billionen Euro im Jahr 2016. Das deutsche Bruttoinlandsprodukt lag im gleichen Jahr bei etwa 2,94 Billionen Euro, Tendenz steigend. Die Zielsetzung der neuen Bundesregierung müsste also höher liegen, um Europa hinsichtlich Cybersicherheit wegweisend zu gestalten.

www.teletrust.de/it-sicherheitsstrategie/
www.teletrust.de/arbeitsgremien/recht/stand-der-technik/
www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit/

► Anforderungen an einen künftigen Europäischen Zertifizierungs- und Kennzeichnungsrahmen für IKT-Sicherheit: TeleTrusT kritisiert Pläne der EU-Kommission und fordert Änderungen

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.

TeleTrusT-Positionen:
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.

ec.europa.eu/transparency/regdoc/rep/1/2017/EN/COM-2017-477-F1-EN-MAIN-PART-1.PDF

► TeleTrusT-Stellungnahme zu Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit

Im Rahmen eines Stellungnahmeverfahrens, das zu Ende 2017 angesetzt war, hat TeleTrusT den DAkkS-Dokumentenentwurf "Akkreditierungsanforderungen für Konformitätsbewertungsstellen im Bereich der Informationssicherheit/Cybersecurity für industrielle Automatisierungssysteme gemäß IEC 62443" kommentiert:

TeleTrusT begrüßt, dass sich die DAkkS mit dem Thema "Cybersecurity für industrielle Automatisierungssysteme" beschäftigt und hierzu auch ein Akkreditierungsschema einfordert. Dies ist im Zuge der Entwicklung des Industrial Internet of Things (IIoT) oder des deutschen Ansatzes "Industrie 4.0" dringend nötig und hilft, "Security by Design" in diesem Umfeld zu forcieren und hinsichtlich der Wirksamkeit in der Umsetzung zu prüfen. TeleTrusT hat aber Bedenken, ob die IEC 62443 in der aktuellen Version zu dem Thema "Cybersecurity für industrielle Automatisierungssysteme" verwendet werden sollte. Hierfür werden folgende Gründe genannt:

- Die aus der ISA99 abgeleitete IEC 62443 ist als Leitfaden für traditionelle Industriesysteme anwendbar, die bisher erstellten Konzepte sind jedoch aus Sicht von TeleTrusT nicht ausreichend für Fragestellungen, die sich aus IIoT bzw. "Industrie 4.0" ergeben, spezifiziert. Eine Verlinkung zu der neuen Referenzarchitektur des BMWi (RAMI) fehlt gänzlich, ebenso mögliche Hinweise zu modernen Konzepten wie "Sensor-to-Cloud" oder Ansätzen aus der deutschen Industrial Data Space Association.
- Teile der IEC 62443 sind derzeit im Status Working Draft - auch die in der Beschlussfassung in der Tabelle 1 aufgeführten Dokumente IEC 62433-3-2, IEC 62443-4-1, IEC 62443-4-2
- Prüfkriterien, wie ein Prüfer speziell gemäß der Normenteile IEC 62443-3-x und IEC 62443-4-x zu prüfen hat, sind derzeit nicht existent und auch nicht ansatzweise vorhanden.

TeleTrusT regt folgende Änderungen an:

1. Motivation: Die Festlegung von Prüf- und Akkreditierungsschemata in Bezug auf "Cybersecurity für industrielle Automatisierungssysteme" ist dringend geboten. Das Thema ist jedoch durch die unterschiedliche Prägung in verschiedenen Sektoren und Branchen sehr fragmentiert. In der Einleitung des Dokumentes fehlt die Würdigung der notwendigen unterschiedlichen Ausprägungen. Ein Bezug auf die Unterschiede zu Fertigungs- und Automatisierungstechnik sowie Verfahrenstechnik und deren unterschiedliche Security-Anforderungen sollte aufgenommen werden, so dass die Eignung der Norm IEC 62443 zur Bewertung dieser unterschiedlichen Security-Anforderungen aufgezeigt wird.

2. Bezug zur aktuellen Gesetzgebung: Kritische Infrastrukturbetreiber (KRITIS), die dem IT-Sicherheitsgesetz, dem EnWG (IT-Sicherheitskatalog), aber auch dem Gesetz zur Digitalisierung der Energiewende oder der Europäischen NIS Directive unterliegen, nutzen industrielle Automatisierungssysteme. Es wäre

wünschenswert, wenn in den Akkreditierungsanforderungen ausführlich Bezug auf das Thema KRITIS genommen und ein Bezug zu den dort bereits genutzten Standards und Normen aufgeführt würde.

3. Abgrenzung und Bezug zu anderen IT-Sicherheitsnormen: Zu dem Thema "Cybersecurity für industrielle Automatisierungssysteme" und die in diesen eingesetzten IT-Security-Komponenten gibt es neben sektorspezifischen Anforderungen der ISO/IEC 270xx-Familie bereits eine Vielzahl weiterer Normen und Standards, wie z.B.:

   a. IEC 62351
   b. VDI/VDE-Richtlinie 2182: Informationssicherheit in der industriellen Automatisierung
   c. NA 115: IT-Sicherheit für Systeme der Automatisierungstechnik
   d. VGB S175: IT-Sicherheit für Erzeugungsanlagen
   e. NIST SP 800-82: Guide to Industrial Control Systems Security
   f. IEEE 1686-2007 - IEEE Standard for Substation Intelligent Electronic Devices (IEDs) Cyber Security Capabilities
   g. BSI: Industrial Control System Security Compendium
   h. OWASP
   i. Common Criteria (ISO 15408)
   j. FIPS 140-2

   Diese Normen und Standards sind bereits vollständig erarbeitet, etabliert und haben zum Großteil auch eigene Prüfverfahren festgelegt. Es wäre vorteilhaft, wenn die DAkkS darlegen würde, warum einer noch nicht fertiggestellten Norm ohne definiertem Prüfverfahren wie der IEC 62443 zur Bewertung der Cybersecurity Vorzug gegenüber den bereits vollständig erarbeiteten und anerkannten Normen gegeben wird.

4. Detaillierte Ausführung der Prüfverfahren oder Verweis auf bestehende Prüfverfahren: Es wird vorgeschlagen, dass bei Feststellung der besseren Eignung der bisher erstellten IEC 62443 die Detailtiefe der Prüfverfahren spezifiziert wird oder auf andere Prüfverfahren referenziert wird, um so dem Mangel der fehlenden bzw. unvollständigen Prüfverfahren in der IEC 62443 entgegenzuwirken. Ansonsten ist für ein Prüfunternehmen nicht ersichtlich, wie die anzusetzende Prüftiefe sein soll (speziell im Hinblick auf den in IEC 62443 aufgeführten Security Level -SL), welche konkreten Methoden und Tools für unterschiedliche Sicherheitsfunktionalitäten verwendet werden sollen und wie eine homogene Interpretation der Prüfergebnisse erfolgen soll. Im schlechtesten Fall wären die Prüfergebnisse beliebig und zueinander weder harmonisiert noch vergleichbar und somit wertlos. Beispielsweise wäre es empfehlenswert, in der Objektklasse "Systeme" genau festzulegen, wie Penetrationstests durchgeführt werden und wie die Qualifikation stattzufinden hat. Man sollte auch darauf verweisen, wie dies im Zuge von Konformitätstests in der Office IT bisher bei der DAkkS geregelt ist. Auch im ICS Security Compendium des BSI finden sich Hinweise auf adäquate Prüfmethoden für die Objektklasse "Systeme". In der Objektklasse "Komponenten" gäbe es die Möglichkeit, auf die vier in IEC 62443 definierten unterschiedlichen Komponenten (Host, Embedded, Application, Network) bewährte Prüfverfahren aufzusetzen, wie z.B. die Common Criteria (CC, durch entsprechend spezifizierte Protection Profiles - PP). In diesem Fall würde man sowohl auf die IEC 62443-4-2 (durch das PP) als auch durch die CC-Methodik implizit die IEC 62443-4-1 hinreichend berücksichtigen.

www.teletrust.de/publikationen/stellungnahmen

► Aktivitäten im politischen Raum mit TeleTrusT-Beteiligung (Auswahl)

■ 16.01.2017, Berlin: SPD-Fachgespräch

■ 01.02.2017, Berlin (BMWi): 2. Erörterungstermin "Verantwortung für IT-Sicherheit im IT-Bereich" Erörterungsgegenstand sind Handlungsoptionen der Bundesregierung und der Unternehmen in Bezug auf den Umgang mit IT-Sicherheitsrisiken im TK-Bereich.

■ 21.02.2017, Bonn (BMBF): Abstimmungsgespräch der deutschen Teilnehmer in den Gremien der European CyberSecurity Organisation (ECSO)

■ 2017-02: "Regulierung des IKT-Marktes in China"

Erörterungs- und Anhörungsverfahren des BMWi zu aktuellen IKT-Regulierungsentwürfen in China
Umfrageverfahren des BMWi, Referat VI A 4

■ 2017-03: "Zielmarktpräferenzen" (BMWi-Exportinitiative Sicherheitstechnologien/KMU-Markterschließungsprogramm)
Umfrageverfahren des BMWi, Referat IV A 4

■ 08.03.2017: "Politische Ziele und Arbeitsweisen von Verbänden"
Mitwirkung im Rahmen eines Forschungsprojektes der Universität Stuttgart, Institut für Sozialwissenschaft, Abteilung für politische Systeme und politische Soziologie

■ 10.03.2017, Berlin: "BSI im Dialog", Veranstaltung in Kooperation mit der Stiftung Datenschutz
Diskussion aktueller Themen der IT-Sicherheit mit BSI-Vizepräsident Dr. Gerhard Schabhüser, der Bundesdatenschutzbeauftragten Andrea Voßhoff und zahlreichen Vertretern von Verbänden, Institutionen und Unternehmen

■ 21.03.2017, Hannover (CeBIT): TeleTrusT/VOICE-"Manifest zur IT-Sicherheit"
Übergabe an BMI und BMWi (u.a. BMI-Staatssekretär Klaus Vitt, IT-Beauftragter der Bundesregierung, Andreas Könen, Leiter Stabsstelle "IT- und Cybersicherheit, sichere IT" im BMI, Arne Schönbohm, BSI-Präsident); www.teletrust.de/it-sicherheitsstrategie/manifest-it-sicherheit

■ 22.03.2017, Brüssel: Konstituierung des ECSO-Strategie- und Koordinierungskomitees
Gerd Müller (secunet/TeleTrusT) wurde als TeleTrusT-Vertreter mit den zweitmeisten Stimmen von 9 Kandidaten in das Strategie- und Koordinierungskomitee der European Cyber Security Organisation (ECSO) gewählt. Das Komitee koordiniert die Arbeiten der Arbeitsgruppen und bereitet Strategieentscheidungen für das ECSO Board of Directors vor (in dem TeleTrusT als ECSO-Gründungsmitglied ebenfalls vertreten ist).

■ 28.03.2017, Berlin: Referentenentwurf des BMI zur Änderung der "Ersten Verordnung zur Änderung der BSI-Kritis-Verordnung"
Verbändeanhörung

■ 31.03.2017, Berlin (BMWi): "Die Rolle der Normung 2030 und Gestaltungsoptionen unter Berücksichtigung der technologiespezifischen Besonderheiten der IKT in der Normung und Standardisierung"

■ 15.05.2017, Berlin: Gespräch mit MdB Saskia Esken (SPD) zur IT-Sicherheitspolitik
- IT-Sicherheitspositionen der SPD-Fraktion
- Erstellung des Regierungsprogramms der SPD für die BT-Wahl 2017
- Verschlüsselung im Spannungsfeld zwischen Sicherheit und staatlichem Eingriffsinteresse
- Ausbildung/Nachwuchsförderung bei IT-Sicherheit
- Sinnhaftigkeit eines "Ministers für Digitales"
- Industrieförderung
- Haftung für unsichere IT-Produkte
- Datenschutzgesetzgebung

■ 08.06.2017, Berlin: BMWi
Erörterungsrunde zum Europäischen Verteidigungsaktionsplan und diesbezüglichen deutschen Beteiligungsmöglichkeiten

■ 20.06.2017, Berlin: eco
Politische Konsultations- und Diskussionsveranstaltung "Vertrauen und Sicherheit im Netz" (Panelteilnehmer Prof. Dr. Pohlmann, TeleTrusT-Vorsitzender)

■ 28.06.2017, Essen: TeleTrusT/Hexatrust (FR)
Verbandspolitische Abstimmungsrunde mit französischem Partnerverband
Hexatrust ist ein TeleTrusT ähnlicher Verband von IT-Sicherheitsunternehmen in Frankreich. Anlässlich der Begegnung, die eine Fortsetzung früherer Gespräche war, wurde nunmehr die Partnerschaft beider Verbände formell etabliert.

■ 2017-06: Evaluierung des Auslandsmesseprogramms des Bundes (BMWi/BAFA)

■ 07.07.2017, Berlin: BMI
Gemeinsame Veranstaltung des Bundesministeriums der Justiz und für Verbraucherschutz, des Bundesministeriums für Wirtschaft und Energie und des Bundesministeriums des Innern zur Einführung eines Gütesiegels für IT-Sicherheit

■ 10.07.2017, Berlin: BMWi
Diskussion der Zwischenergebnisse des BMWi/DIN-Projektes "Sichere Digitale Identitäten" und Beiratssitzung

■ 11.07.2017, Brüssel: EU-Kommission/DIN
"How does standardization support IT Security in the Digital Single Market?"
(Panelisten: Dr. Andreas Schwab, Mitglied des Europäischen Parlamentes und Berichterstatter der NIS Richtlinie, Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation, Bernd Kowalski, Abteilungsleiter im BSI, Markus Reigl, Direktor für Technische Regulierung und Normung bei Siemens sowie Jean-Pierre Quémard, Vorsitzender der Cyber Security Coordination Group.)

■ 24.08.2017, Berlin: BMI
Erörterungsgespräch mit Andreas Könen, BMI, zum Thema "Bundestrojaner"

■ 30.08.2017, Düsseldorf: Thomas Jarzombek (CDU)
Erörterungsgespräch zu aktuellen Fragen der IT-Sicherheitspolitik

■ 31.08.2017, Berlin, Spanische Botschaft, Wirtschafts- und Handelsbüro
Erörterungsgespräch zu Möglichkeiten der Kooperation auf dem Gebiet IT-Sicherheit

■ 07.09.2017, Bonn: BMWi
Ergebnis-Präsentation und Workshop-Diskussion zu BMWi-Studie "Hemmnisse beim Einsatz elektronischer Verschlüsselung"

■ 03.10.2017, Brüssel
ENISA: Industry Network event "Business opportunities arising from EU regulation"

■ 06.10.2017, Berlin
Jimmy Schulz (FDP): Erörterungsgespräch zu aktuellen Fragen der IT-Sicherheitspolitik

■ 15.11.2017, Bonn
BMFT: Zusammenkunft deutscher Beteiligter an ECSO und ECS cPPP

■ 29.11.2017, Berlin
Digital Business Connectivity - Deutsch-Koreanische Kooperation in den Bereichen IKT und Smart Services

■ 30.11.2017, Berlin
"Perspektiven der IT-Sicherheit in Deutschland" (Erörterungsgespräch TeleTrusT, VOICE, BMWi)

■ 07.12.2017, Berlin
BMWi: Anhörung zu den Auswirkungen des chinesischen Cybersicherheitsgesetzes auf deutsche Unternehmen

► TeleTrusT-Präsenz (Auswahl)

■ BSI-Kongress
■ Jahrestagung des Berufsverbandes der Datenschutzbeauftragten
■ Deutsch-Indisches Wirtschaftsforum
■ "69 Jahre Israel", Networking-Empfang
■ CEN CENELEC Cybersecurity Co-ordination Group
■ CommunicAsia
■ ECSO Board Meetings

- Omnisecure-Beiratssitzung
- "Infosecurity" (London)
- TREATS-Workshop "eIDAS-Erweiterungen für eID-Szenarien"
- DIHK-Politikerpanel zu IT-Sicherheitsfragen
- TaylorWessing: "EU-Datenschutzgrundverordnung"

2 Ausgewählte Themen

► T.I.S.P.-Beirat konstituiert

TeleTrusT hatte innerhalb des T.I.S.P.-Absolventenkreises zu Interessenbekundungen für einen "T.I.S.P.-Beirat" aufgerufen. Basierend auf den Rückmeldungen wurde am 10.01.2017 auf Beschluss des T.I.S.P.-Lenkungsgremiums dieser Beirat konstituiert und die nachstehenden Experten berufen:

Patrick Sauer, bisec GmbH, Frankfurt am Main
Thomas Floß, EDV-Unternehmensberatung Floß, Versmold
Holger Westphal, ivv GmbH, Hannover
Gerald Scheer, Fiducia & GAD IT AG, Münster.

Der Beirat wird in dieser Zusammensetzung zunächst befristet bis 31.12.2018 als fachliches Beratungsgremium für die inhaltlich-thematische Fortentwicklung des T.I.S.P.-Curriculums sowie für die Programmgestaltung des jährlichen T.I.S.P. Community Meetings tätig.

Der T.I.S.P. ist ein deutschsprachiges Expertenzertifikat für IT-Sicherheitsfachleute. Die Inhalte, die für das T.I.S.P.-Zertifikat relevant sind, umfassen die wichtigsten internationalen Standards der Informationssicherheit und berücksichtigen darüber hinaus die Prinzipien des IT-Grundschutzes sowie die deutsche und europäische Gesetzgebung. TeleTrusT ist Träger des T.I.S.P.

www.teletrust.de/tisp/

► TeleTrusT-Handreichung zum Umgang mit der Blockchain

Die kryptographische Währung Bitcoin und die als Blockchain bekannte dahinterstehende Technologie sind aktuelle Hype-Themen, jedoch inhaltlich einem breiteren Publikum noch weitgehend unbekannt. TeleTrusT hat deshalb eine Handreichung zum Umgang mit der Blockchain veröffentlicht. 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. Praktische Anwendungsfälle mit Bezug zu IT-Sicherheit sind daher zentrales Thema. Oftmals wird die Blockchain mit Bitcoin auf eine sehr spezielle Anwendung reduziert. Im Fokus der TeleTrusT-Publikation steht daher das Potential der Blockchain-Technologie insgesamt. Die TeleTrusT-Handreichung zeigt auf, welche Anwendungen von Blockchains profitieren können und für wen diese Anwendungen dann praktischen Nutzen entfalten. Dabei können am Ende sowohl komplett offene Anwendungsfälle als auch Anwendungen für geschlossene Nutzergruppen in Betracht kommen. Exemplarisch wird dies im Umfeld von elektronischen Identitäten und Zugriffskontrollmechanismen dargestellt.

Dr. André Kudra, Leiter der TeleTrusT-Arbeitsgruppe "Blockchain", sieht gute Chancen für eine Verbreitung der Technologie und damit für die IT-Sicherheitswirtschaft: "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".

Die TeleTrusT-"Handreichung zum Umgang mit der Blockchain" ist unter www.teletrust.de/publikationen/broschueren/blockchain/ verfügbar.

► German Brand Award für TeleTrusT-Vertrauenszeichen "IT Security made in Germany"

Das TeleTrusT-Vertrauenszeichen "IT Security made in Germany" des Bundesverbandes IT-Sicherheit e.V. wurde durch den Rat für Formgebung (German Design Council) und das German Brand Institute mit dem German Brand Award 2017 in der Kategorie "Industrial Excellence in Branding" ausgezeichnet.

Unter dem TeleTrusT-Vertrauenszeichen "IT Security made in Germany" wird die gemeinsame Außendarstellung der organisierten deutschen IT-Sicherheitswirtschaft koordiniert, die Zusammenarbeit gefördert und deutsche Industriekompetenz in einschlägigen Exportmärkten markiert. Die Verwendung des als Marke geschützten Zeichens wird deutschen IT-Sicherheitsunternehmen auf der Basis von bestimmten Fachkriterien, zu deren Einhaltung sich die Unternehmen verpflichten müssen, gestattet.

Die Initiative "IT Security made in Germany" wurde ursprünglich mit Begleitung des Bundeswirtschaftsministeriums und des Bundesinnenministeriums durch die deutsche IT-Sicherheitswirtschaft etabliert. Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) übernahm 2011 die Trägerschaft.

Mit der Verleihung des German Brand Award an die TeleTrusT-Marke "IT Security made in Germany" wurde sowohl das nachhaltige industriepolitische Engagement der organisierten deutschen IT Security als auch die Stringenz in der Markenpflege durch TeleTrusT anerkannt.

Die Auszeichnung wurde am 29.06.2017 in Berlin an TeleTrusT überreicht.

www.teletrust.de/itsmig/

► TeleTrusT-Koordinierungskreis "ECSO" etabliert

TeleTrusT ist Gründungsmitglied der European Cybersecurity Organisation (ECSO), im ECSO Board of Directors vertreten und wirkt mit Experten in verschiedenen ECSO-Arbeitsgruppen mit. Um das deutsche bzw. TeleTrusT-Engagement zu koordinieren, wurde anlässlich einer Sitzung am 31.08.2017 ein TeleTrusT-Koordinierungskreis "ECSO" etabliert. Leiter ist Gerd Müller (secunet), zugleich auch für TeleTrusT im ECSO Board bzw. dortiger Vice Chairman.
Ergebnisse der Zusammenkunft:

■ Die Frage nach einem TeleTrusT- bzw. deutschen Engagement in ECSO wurde einstimmig positiv beantwortet. Mit Blick auf die deutliche Präsenz anderer Länder wird eine Ausweitung als geboten erachtet.
■ TeleTrusT wird als geeignete Koordinierungsplattform betrachtet. Die Plattform ist anlassbezogen offen für Gäste, insbesondere aus den Ressorts BMI und BMWi.
■ Aus Sicht von TeleTrusT bzw. des Koordinierungskreises besteht kein Interesse daran, die etablierten und bewährten Zeichen wie z.B. "IT Security made in Germany" und "TeleTrusT Information Security Professional" durch ein europäisches Zeichen überlagern, konterkarieren oder verwässern zu lassen.
■ Mittels des TeleTrusT-KK "ECSO" wird die Benennung von Experten für ECSO Working Groups und die konsolidierte Meinungsbildung erfolgen.

► TeleTrusT-Innovationspreis 2017 für Steen Harbach AG

Der TeleTrusT-Innovationspreis 2017 wurde an die Steen Harbach AG Leverkusen für die IT-Sicherheitslösung "Real end-to-end security for IoT devices & Industry 4.0" vergeben. Die Preisübergabe erfolgte am 14.11.2017 im Rahmen des T.I.S.P. Community Meetings in Berlin. Den Preis nahmen Witali Bartsch (VP Security Solutions), Arash Emami (Security Engineer) und Joachim Wülbeck (Product Manager) für Steen Harbach entgegen.

Nominiert für den TeleTrusT-Innovationspreis 2017 waren aus insgesamt 21 Einreichungen auch Lösungen von certgate, Governikus, HID, HPI, Rhebo und Secorvo.

► "Cyber Security Challenge Germany": Unternehmenspräsentation, Nachwuchs-Recruiting, Networking

Die diesjährige "Cyber Security Challenge Germany" (CSCG) richtete sich erneut an Schüler und Studenten. Mit der CSCG soll das inländische Qualifikationspotential in der IT-Sicherheit ermittelt und zugleich gefördert werden. Zunächst wurden am 04. und 05.07.2017 die besten "Nachwuchshacker" Deutschlands ermittelt. Der europäische Ausscheid wird vom 30.09. - 02.10.2017 in Spanien stattfinden.

TeleTrusT-Vorsitzender Prof. Pohlmann hielt die Begrüßungsansprache und übergab zusammen mit TÜViT-Geschäftsführer Dirk Kretzschmar die Preise an die Gewinner.

Interessierte Unternehmen hatten Gelegenheit, die Talente beim Landesfinale zu unterstützen und sich als potentieller Arbeitgeber zu präsentieren. Diese Kurzvorstellung der beteiligten IT-Sicherheitsunternehmen und -institutionen wurde von TeleTrusT organisiert und ermöglichte die direkte Ansprache des IT-Sicherheitsnachwuchses. Die anschließende Siegerehrung lud zudem zum Austausch mit Experten der Branche ein.

In der "Cyber Security Challenge Germany" werden Schüler und Studenten mit realistischen Cyber-Angriffen konfrontiert und vor Herausforderungen gestellt. Im Zusammenwirken von Politik, Wirtschaft, Forschung und Fachmedien werden gezielt junge Talente angesprochen und motiviert. Die Sieger messen sich mit den Besten aus Europa auf einer Abschlussveranstaltung. Die CSCG ist ein gemeinsames Projekt von TeleTrusT, dem Institut für Internet-Sicherheit if(is) an der Westfälischen Hochschule und der Heise Medien GmbH & Co. KG.

www.cscg.de/
www.teletrust.de/cyber-security-challenge/2017-germany/

► Marktforschungsverbände in Kooperation mit TeleTrusT: ISO-Norm für Internetanalysen in der Markt-, Meinungs- und Sozialforschung

ISO 19731 "Digital analytics and web analyses for purposes of market, opinion and social research - Vocabulary and service requirements" ist eine neue Norm für die Markt-, Meinungs- und Sozialforschung im Internet. Die Norm stellt Anforderungen an "good research practice" bei web-basierten Analysen. Erarbeitet wurde ISO 19731 in Kooperation mit TeleTrusT von den deutschen Marktforschungsverbänden ADM und DGOF mit den Partnerverbänden aus Österreich, Großbritannien, Spanien, Japan, Kanada, den USA und den Niederlanden sowie EFAMRO und ESOMAR. Das deutschsprachige Begleitgremium wurde unter dem Dach von Austrian Standards organisiert. Die Entwicklung der Norm begann im Februar 2014 und wurde im November 2016 mit breitem Grundkonsens abgeschlossen. Die Norm trat Anfang 2017 in Kraft.

►TeleTrusT/Beuth-Sonderdruck ISO 19731 "Digital analytics and web analyses"

Die Digitalisierung ist auch für die Markt- und Sozialforschung prägend. Dies kennzeichnet folgerichtig die einschlägige Normung. ISO 19731 "Digital analytics and web analyses for purposes of market, opinion and social research - Vocabulary and service requirements" ist eine neue, innovative Norm für die internetbasierte Markt-, Meinungs- und Sozialforschung im Internet. Die Norm stellt Anforderungen an "good research practice" bei web-basierten Analysen. Erarbeitet wurde ISO 19731 in Kooperation mit TeleTrusT von den deutschen Marktforschungsverbänden ADM und DGOF (TeleTrusT-Mitglied bzw. Partnerverband) mit den Branchenverbänden aus Österreich, Großbritannien, Spanien, Japan, Kanada, den USA und den Niederlanden sowie den Dachverbänden EFAMRO und ESOMAR. Die Entwicklung der Norm wurde mit breitem Grundkonsens der Branche abgeschlossen.

TeleTrusT und der dem DIN Deutsches Institut für Normung angeschlossene Beuth-Verlag haben einen Sonderdruck der ISO 19731 aufgelegt, der in limitierter Stückzahl über TeleTrusT verfügbar ist.

3 Veranstaltungen

► Interner Workshop der Schulungsanbieter zum "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.)

Die Schulungsanbieter für das TeleTrusT-Expertenzertifizierungsprogramm "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) führten am 11. und 12.01.2017 in Karlsruhe bei Gastgeber secorvo einen internen Workshop durch, bei dem die Aktualisierung und die Fortentwicklung der Lehr- und Prüfungsinhalte des T.P.S.S.E.-Syllabus erörtert wurde.

www.teletrust.de/veranstaltungen/tutorials-workshops/tpsse-workshop/

► TeleTrusT als Partner der OMNISECURE 2017

TeleTrusT war Partner der OMNISECURE vom 16.01. bis 18.01.2017 in Berlin (früherer Veranstaltungstitel: OMNICARD). Die OMNISECURE führt jährlich die wesentlichen Akteure aus Industrie und Politik zusammen. Geplant sind an zwei Kongresstagen 70 Referenten, 22 Foren, 12 Workshops für interdisziplinäre Fachdiskussionen. Im Mittelpunkt stehen die Themen Internet of Things, Smart Home, Blockchain, eIDAS, Industrie 4.0 und FIDO sowie die einschlägige Regulierung. Die Schirmherrschaft hat das Bundesministerium des Innern übernommen. Die Teilnahmekonditionen, insbesondere für Wissenschaft und Behörden, wurden verbessert.

► Interner Workshop der TeleTrusT-AG "SICCT"

Die TeleTrusT-AG "SICCT" (SICCT = Secure Interoperable ChipCard Terminal") führte am 19.01.2017 in Berlin einen AG-internen Workshop durch, bei dem Inhalte und Strategien für die Fortentwicklung der bestehenden TeleTrusT-SICCT-Spezifikation erörtert wurden.

www.teletrust.de/veranstaltungen/tutorials-workshops/interner-workshop-der-teletrust-ag-sicct/
www.teletrust.de/projekte/sicct/#c535

► Intersec 2017 in Dubai: TeleTrusT-Gemeinschaftsstand

TeleTrusT und die Messe Frankfurt mit der Landesgesellschaft Middle East kooperierten bei der Präsentation von "IT Security made in Germany" auf der Intersec 2017 in Dubai. Die Intersec ist eine internationale Fachmesse für die Bereiche Kommerzielle Sicherheit, Informationssicherheit, Brandschutz und Rettung, Personenschutz, Gesundheit, Innere Sicherheit und Überwachung. Mit Gemeinschaftsauftritten wie auf der Intersec verfolgt TeleTrusT das Anliegen, gemeinsam mit interessierten Verbandsmitgliedern IT-Sicherheitsprodukte und -Dienstleistungen unter der TeleTrusT-Marke "IT Security made in Germany" vorzustellen. Die 19. Intersec Dubai 2017 fand vom 22.01. bis 24.01.2017 in Dubai, VAE, statt und führte als Messe mit begleitenden Veranstaltungen Entscheider und Verantwortungsträger aus Wirtschaft und Behörden zusammen. Beteiligte TeleTrusT-Mitgliedsunternehmen 2017 waren unter anderem G Data und bc digital.

www.teletrust.de/veranstaltungen/intersec/intersec-2017/

► RSA Conference 2017 in San Francisco: TeleTrusT präsentierte "IT Security made in Germany"

Vom 13.02. bis 17.02.2017 fand in San Francisco, USA, die 26. "RSA Conference" statt. Die RSA San Francisco ist nach wie vor die weltweit führende Messe bzw. Konferenz für IT-Sicherheit mit internationaler Beteiligung. Am "German Pavilion" präsentierte TeleTrusT mit zahlreichen Verbandsmitgliedern "IT Security made in Germany". Der Gemeinschaftsstand wurde zum 17. Mal in Folge mit einer vom Bundesministerium für Wirtschaft und Energie geförderten und von TeleTrusT gestalteten Gemeinschaftsausstellung vertreten. Die Organisation oblag der NürnbergMesse als verantwortlicher Durchführungsgesellschaft. Durch den etablierten Goldsponsor-Status des "German Pavilion" und die damit verbundenen Präsentationsmöglichkeiten ist gewährleistet, dass Besucher und Konferenzteilnehmer auf vielfältige Weise Kenntnis von ausgewählten Leistungsangeboten der deutschen IT-Sicherheitsindustrie nehmen können.

Begleitend zur Standpräsentation organisierte TeleTrusT zusammen mit Verbandsmitgliedern eine Reihe von Begegnungsmöglichkeiten und Fachveranstaltungen.

www.teletrust.de/veranstaltungen/rsa/rsa-2017/

► TeleTrusT Veranstaltungspartner der European Union of Associations of Translation Companies

Die European Union of Associations of Translation Companies (EUATC) richtete am 20. und 21.04.2017 ihren internationalen Jahreskongress in Berlin aus. Die EUATC ist einer der weltweit größten Übersetzerverbände und umfasst als Mitglieder sowohl Einzelübersetzer, kleine bis mittlere Übersetzerbüros als auch größere Übersetzungsunternehmen, die praktisch alle Themen abdecken. Die EUATC ist außer mit Branchenpolitik auch mit EN- und ISO-Standardisierung befasst sowie mit aktuellen Themen wie IT-Sicherheit für Unternehmen, sichere Datenübermittlung z.B. bei sicherheitskritischen Übersetzungsaufträgen und Cloud-Lösungen. Das Netzwerk der EUATC ragt naturgemäß in sehr viele Industrie- und Verwaltungsbereiche hinein.

Im Rahmen einer Veranstaltungskooperation konnte TeleTrusT auf dem EUATC-Kongress zu den Themen

- Cloud Security
- Verschlüsselung
- Sicherer Datenaustausch.

und die aktuelle Gefahrenlage für KMUs referieren. Die Präsentation wurde namens TeleTrusT durch Dr.-Ing. habil. Ralf Rieken (TeleTrusT-Mitglied Uniscon GmbH München) ausgeführt.

► DIN-Akademie: Tagung zu EU-Datenschutzgrundverordnung in Kooperation mit TeleTrusT

Das Deutsche Institut für Normung e.V. (DIN) bzw. die DIN-Akademie in Kooperation mit TeleTrusT führt am 27.04.2017 eine Tagung "Datenschutzgrundverordnung in der Praxis - Umsetzung, Standards, Datenschutzkonzepte und -management" durch.

Den zentralen TeleTrusT-Part übernahm RA Bernhard Kloos (TeleTrusT-Mitglied HK2 RAe) zum Themenkreis Einwilligungsmanagement im Rahmen der EU-DSGVO/Neue Regeln für die Einwilligung von Betroffenen/Umgang mit alten Datenbeständen/Prozess- und Formularumstellungen/Dokumentationspflichten der verantwortlichen Stelle.

► TeleTrusT-Regionalstelle München: itWatch organisierte Regionaltreffen (Rückschau)

Auf Einladung von TeleTrusT-Mitglied itWatch als "TeleTrusT-Regionalstelle München" fand am 12.05.2017 unter reger Beteiligung in München ein Regionalabend statt. Veranstaltungsort war das "Giesinger Bräu". Als Sprecher trat Michael George, Bayerisches Landesamt für Verfassungsschutz, zum Thema "Digitale Industriespionage" auf.

www.teletrust.de/ueber-teletrust/regionalstelle-muenchen/

► Schwerpunkt IT Security/Automotive: TeleTrusT Partner der Cyber Secure Car Europe

TeleTrusT war Partner der Cyber Secure Car Europe am 23. und 24.05.2017 in München. Die Cyber Secure Car richtete sich an Experten und Entscheidungsträger aus "software and hardware engineers from global OEMs, T1s, semiconductor suppliers, embedded software providers, telematics companies and security specialists concerned with safeguarding all aspects of the connected car from external threats."

► TeleTrusT-Informationstag "IT-Sicherheit in der ärztlichen Praxis" am 31.05.2017 in Berlin

Die Gesundheitsversorgung befindet sich im Zuge der Digitalisierung im Umbruch. Unbestreitbar bietet die Digitalisierung enorme Chancen zur Verbesserung von Patientenbehandlung und zur Optimierung von Verwaltungsabläufen. Gleichzeitig steckt darin aber auch ein hohes Missbrauchs- und Gefährdungspotential im Fall von schlechter Datenhaltung oder ungenügend gesicherter Datenübertragung. Der Zugriff nur durch berechtige und qualifizierte Personen muss zu jedem Zeitpunkt sichergestellt sein. Für Ärzte und Personal in Klinik und Praxis sind daher Kenntnis und Nutzung sicherer IT-Systeme unabdingbar. TeleTrusT veranstaltete in Kooperation mit Vertretern der Gesundheitstelematik einen Informationstag zu aktuellen Herausforderungen der IT-Sicherheit für angestellte und niedergelassene Ärzte. Neben Beiträgen aus dem ärztlichen Praxis-Alltag benennen erfahrene Anwender technische, organisatorische und rechtliche Notwendigkeiten und Obliegenheiten. Thematisiert wurde u.a.:

- IT-Sicherheit in Arztpraxen, Visionen und Realitäten
- Digitalisierung in der Medizin: Quo vadis?
- Angewandte Informationssicherheit in der Arztpraxis - Aktueller Stand und Ausblick auf die Telematikinfrastruktur
- Das Recht auf eigene Daten - Juristische Fragestellungen in der digitalisierten Medizin
- Digitale Patientenakten und intersektorale Vernetzung in der täglichen Patientenversorgung
- Big Data im Spannungsfeld von Datenschutz und Auswertungsinteressen.

Eine Paneldiskussion über die Zukunft der digital unterstützen ärztlichen Tätigkeit rundete das Programm ab.

www.teletrust.de/veranstaltungen/aerztliche-praxis

Gemäß Anerkennungsbescheid der Ärztekammer Berlin war die nachgewiesene Teilnahme an dieser Veranstaltung als ärztliche Fortbildungsmaßnahme (CME) anerkennungsfähig.

► TeleTrusT-Regionalstelle Hamburg (WMC): "ITSiG und DSGVO" am 08.06.2017

Die TeleTrusT-Regionalstelle Hamburg, repräsentiert durch Wüpper Management Consulting (WMC), und TeleTrusT lud ein zum 7. Hamburger Regionaltreffen ein. Gastgeber war die Taylor Wessing RAe Partnerschaftsgesellschaft.

Themen:

- Datenschutz-Grundverordnung (DSGVO)
- Stand der Technik im Sinne des IT-Sicherheitsgesetzes
- Umsetzung von IT-Sicherheitsgesetz und DSGVO

► TeleTrusT/EBCA-PKI Workshop 2017

Die Mitglieder des TeleTrusT/EBCA-Lenkungsgremiums und der TeleTrusT-EBCA-AG "Technik" führten am 22.06.2017 in Berlin erneut den TeleTrusT-EBCA-"PKI-Workshop" durch, wo in einem diskussionsfördernden Rahmen aktuelle Themen rund um Public-Key-Infrastrukturen besprochen werden. Auf Basis der durchgehend positiven Rückmeldungen des Vorjahres wurden nach einer Einführung erneut kurze Impulsvorträge gehalten, gefolgt von ausführlichen Workshop-Sessions und der gemeinsamen Betrachtung der

Ergebnisse. Erneut wurden Fragen zu eIDAS beantwortet, neue Standards diskutiert und Projekte vorgestellt.

www.teletrust.de/veranstaltungen/tutorials-workshops/ebca-pki-2017/

Die TeleTrusT European Bridge CA (EBCA) ist ein Zusammenschluss einzelner, gleichberechtigter Public-Key-Infrastrukturen (PKIen) zu einem PKI-Verbund. Sie ermöglicht eine sichere und authentische Kommunikation zwischen den beteiligten Unternehmen, Institutionen und öffentlichen Verwaltungen. Durch die Mitgliedschaft in der EBCA können ausgegebene Zertifikate über lokale "Identitätsinseln" hinaus verwendet werden. Somit werden unterschiedliche Geschäftsprozesse (Secure Email, Secure Logon, Secure eID, etc.) über die Grenzen der einzelnen Organisationen hinweg nutzbar gemacht.

www.ebca.de/

► TeleTrusT-interner Workshop 2017 bei secunet in Essen

Am 29. und 30.06.2017 fand der traditionelle jährliche TeleTrusT-interne Workshop (IWS) statt, zu dem alle Verbandsmitglieder und interessierte Gäste herzlich eingeladen waren. Gastgeber war die secunet Security Networks AG, Essen. Die Veranstaltung richtete sich in erster Linie an TeleTrusT-Mitglieder, aber auch an potentielle TeleTrusT-Interessierte. Im Rahmen des Workshops wurden Impulsvorträge gehalten, gefolgt durch Fachdiskussionen. Der IWS bot Gelegenheit, gemeinsam die fachliche Fortentwicklung des Verbandes zu erörtern:

■ Was sollen und müssen wir als TeleTrusT tun, um Angebot und Nachfrage optimal aufeinander einzustellen?
■ Was sind die Themen, die den IT-Sicherheitsbedarf befriedigen und die IT- Sicherheitsindustrie stärken?
■ Wie sollten wir zusammen vorgehen, um die besten Ziele für die Mitglieder von TeleTrusT zu erreichen?

Leiter und Sprecherinnen der TeleTrusT-Gremien gaben Statusberichte.

www.teletrust.de/veranstaltungen/tutorials-workshops/teletrust-iws-2017/

► "Cyber Security Challenge Germany": Unternehmenspräsentation/Nachwuchs-Recruiting/Networking

04.07.2017 - 05.07.2017, Düsseldorf

Die "Cyber Security Challenge Germany" (CSCG) richtete sich erneut an Schüler und Studenten. Mit der CSCG soll alljährlich das inländische Qualifikationspotential in der IT-Sicherheit ermittelt und zugleich gefördert werden. Zunächst wurden am 04. und 05.07.2017 die besten "Nachwuchshacker" Deutschlands und anschließend im Herbst die talentiertesten "Junghacker" Europas ermittelt. Interessierte Unternehmen haben dabei Gelegenheit, die Talente beim Landesfinale zu unterstützen und sich als potentieller Arbeitgeber zu präsentieren. Am 05.07.2017 in Düsseldorf traf eine hochqualifizierte Zielgruppe aus jungen IT-Security-Talenten zusammen. Die Kurzvorstellung der beteiligten IT-Sicherheitsunternehmen und -institutionen wurde von TeleTrusT organisiert und ermöglichte die direkte Ansprache des IT-Sicherheitsnachwuchses. Die anschließende Siegerehrung lud zudem zum Austausch mit Experten der Branche ein.
In der "Cyber Security Challenge Germany" werden Schüler und Studenten mit realistischen Cyber-Angriffen konfrontiert und vor Herausforderungen gestellt. Im Zusammenwirken von Politik, Wirtschaft, Forschung und Fachmedien werden gezielt junge Talente angesprochen und motiviert. Die Sieger messen sich mit den Besten aus Europa auf einer Abschlussveranstaltung.

Die CSCG ist ein gemeinsames Projekt von TeleTrusT, dem Institut für Internet-Sicherheit if(is) an der Westfälischen Hochschule und der Heise Medien GmbH & Co. KG. Das Projekt wurde bis 2016 durch das Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative "IT-Sicherheit in der Wirtschaft" unterstützt.

www.cscg.de/
www.teletrust.de/cyber-security-challenge/

► Blockchain in der Praxis: TeleTrusT-Informationstag mit Anwendungsszenarien

Die Blockchain verdankt ihre Bekanntheit der kryptografischen Währung Bitcoin. Mit wachsender Verbreitung rücken weitere Anwendungsmöglichkeiten in den Fokus. TeleTrusT veranstaltete am 13.07.2017 in Frankfurt am Main den TeleTrusT-Informationstag "Blockchain", um das Thema mit Blick auf praktische Anwendbarkeit zu behandeln.

Der TeleTrusT-Informationstag "Blockchain" betrachtete bereits bestehende oder konzeptionierte "Blockchain use cases", um den Fortschritt auf diesem Gebiet zu betrachten.

www.teletrust.de/veranstaltungen/blockchain/

Für den Einstieg in das Thema hat die TeleTrusT-Arbeitsgruppe "Blockchain" eine Handreichung veröffentlicht, die Interessierten erste Anwendungen bzw. Konzepte näherbringt. Exemplarisch wird dies im Umfeld von elektronischen Identitäten und Zugriffskontrollmechanismen dargestellt. Die TeleTrusT-"Handreichung zum Umgang mit der Blockchain" ist unter www.teletrust.de/publikationen/broschueren/blockchain/ abrufbar.

► TeleTrusT Veranstaltungspartner der ditact "Women´s IT Summer Studies" der Universität Salzburg

Die Universität Salzburg als Hauptträgerin und die Fachhochschule Salzburg lud IT-Fachfrauen ein, Lehrangebote für die 15. ditact "Women´s IT Summer Studies" einzureichen, die vom 21.08. - 02.09.2017 stattfand. TeleTrusT unterstützte diese Aktivität. Die Lehre umfasste auch ein Modul "IT-Sicherheit". Das Angebot richtete sich an "Fachfrauen" in der IT bzw. IT-Sicherheit.

Die ditact bietet einerseits Frauen die Möglichkeit, eine spezialisierte akademische Weiterbildung im Informatik- bzw. IT-Sektor zu erhalten und andererseits Erfahrungen in der Lehre zu sammeln.

► TeleTrusT/VOI-Informationstag und Workshop "Elektronische Signatur" 2017

TeleTrusT und der TeleTrusT-Partnerverband Organisations- und Informationssysteme e.V. (VOI) ermöglichten auf dem Informationstag und Workshop "Elektronische Signatur" am 20.09.2017 in Berlin einen intensiven Austausch bei Gruppenarbeiten und persönlichen Gesprächen. Experten aus Wirtschaft, Verwaltung und Forschung erörtern in Impulsvorträgen die aktuelle Situation der elektronischen Signatur und stoßen Diskussionen an.

Mit der Veranstaltungsreihe wird jährlich eine Plattform geboten, auf der neben den neuesten Informationen rund um die elektronische Signatur vor allem der Austausch mit den Teilnehmern im Vordergrund steht.

Themen (Auszug):

- Status VDG Vertrauensdienstegesetz / Vertrauensdiensteverordnung
- eIDAS-Marktbetrachtung / Spaltung und Fusion des 'eIDAS-Atoms' - insb. starke Authentikation
- Elektronische Siegel: Grundlagen, Recht, Technische Umsetzung, individuelle Anwendungsszenarien
- Internationale Signaturanwendungen und Registrierungsprozesse / Rechtskonforme Vertragsabschlüsse
- "eSig Matchmaking"

www.teletrust.de/veranstaltungen/signaturtag/infotag-elektronische-signatur-2017/

► TeleTrusT-Regionalstelle Mannheim (SAMA PARTNERS): Regionaltreffen am 28.09.2017

Die TeleTrusT-Regionalstelle Mannheim, repräsentiert durch Sama Partners, lud in Kooperation mit TeleTrusT zum 1. Regionaltreffen nach Mannheim ein.

Vortragsthemen:

■ Die Bedeutung von IT-Sicherheit im digitalen Zeitalter
■ Herausforderung Mensch & Mobile Sicherheit
■ Vertrauenswürdige IT- und Netz-Infrastrukturen durch Blockchain

► TeleTrusT als Partner des IT-GRC-Kongresses

TeleTrusT war Partner des IT-GRC-Kongresses am 28. und 29.09.2017 in Berlin. Namens TeleTrusT konnten TeleTrusT-Vorsitzender Prof. Dr. Norbert Pohlmann und TeleTrusT-Vorstand RA Karsten U. Bartels mit Vorträgen vertreten sein:

► TeleTrusT + Cluster Automation & Mechatronik: Workshop zu "Industrial Security" in Crailsheim

Auch 2017 konnte TeleTrusT in Kooperation mit dem Bayerischen "Cluster Automation & Mechatronik" einen Herbst-Workshop zu "Industrial Security" durchführen. Die Teilnehmer erhielten einen Überblick über die aktuelle Entwicklung im Bereich Forschung für die industrielle Sicherheit, über Herausforderungen der Industrieunternehmen und über aktuelle Lösungsansätze. Die Veranstaltung ermöglichte neben Networking einen Überblick über IT-Lösungen für die Automation, neue Gefahren durch Cyberattacken und "Best-Practice"-Lösungsansätze.

www.teletrust.de/veranstaltungen/tutorials-workshops/industrial-security-2017/

► TeleTrusT auf it-sa 2017: Blockchain, IT-Sicherheitsgesetz, Deutsch-Französischer Workshop

TeleTrusT beteiligte sich als Veranstaltungspartner aktiv an der nationalen Leitmesse für IT-Sicherheit it-sa vom 10. - 12.10.2017 in Nürnberg. Die it-sa bot Gelegenheit zum Meinungsaustausch und informierte über einschlägige Produkte und Dienstleistungen. Neben den Themen Blockchain, Mobile Security, Verschlüsselung, IT Compliance und Biometrie fanden Netzwerksicherheit, IT-Grundschutz und das IT-Sicherheitsgesetz breite Präsentationsfläche. TeleTrusT ist seit Gründung der it-sa Veranstaltungspartner. Die NürnbergMesse als Trägergesellschaft ist TeleTrusT-Mitglied.

www.teletrust.de/veranstaltungen/it-sa/it-sa-2017/

■ TeleTrusT-Auditorium "Blockchain - Anwendungsszenarien"
■ TeleTrusT-Vortrag zu IT-Sicherheitsgesetz/Stand der Technik
■ Deutsch-Französischer Workshop: "IT Security in Germany and France - Opportunities for co-operation" (www.teletrust.de/veranstaltungen/tutorials-workshops/deutsch-franzoesischer-workshop/)

■ it-sa-Messeparty (Am 11.10.2017 fand nach Messeschluss die it-sa-Messeparty mit TeleTrusT als Mitträger statt.)

Eingeleitet wurde die "it-sa-Woche" mit dem "Security Summit", organisiert von TeleTrusT-Mitglied qSkills, eine von TeleTrusT mitgetragene Veranstaltung (09.10.2017, Nürnberg)

► TeleTrusT/BvD: IT-Sicherheitsrechtstag 2017 in Berlin

Wie gestalten Unternehmen ihr Datenschutzmanagement bereits mit Blick auf die ab Mai 2018 in der EU wirksame Datenschutz-Grundverordnung rechtssicher? Welche Anforderungen stellen die Aufsichtsbehörden an den Datenschutz? Was bedeutet "Stand der Technik"? Worauf ist bei Datenschutz-Auditierungen zu achten? Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) und der Berufsverband der Datenschutzbeauftragten Deutschlands e.V. (BvD) gaben im Rahmen einer Informationsveranstaltung am 07.11.2017 in Berlin praktische Anleitung.

Aus dem Programm:

■ Herausforderung EU-Datenschutz-Grundverordnung - Ein Bericht aus der Praxis
■ Der betriebliche Datenschutzbeauftragte in der DSGVO
■ Wenn die Aufsichtsbehörde klingelt: Wie läuft eine Prüfung ab?
■ Implementierung gesetzlicher IT-Sicherheitsmaßnahmen nach DSGVO und IT-Sicherheitsgesetz
■ Maßnahmenermittlung nach dem Stand der Technik
■ DSGVO - Vorgehensweise zur Umsetzung am Praxisbeispiel enercity (Stadtwerke Hannover AG)
■ Datenschutz-Auditierung

www.teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dsgvo/2017/

► TeleTrusT als Partner der 20. Berner Tagung für IT-Sicherheit

TeleTrusT war Partner der 20. Berner Tagung für IT-Sicherheit am 23.11.2017 in Bern, CH, ausgerichtet durch den Schweizer TeleTrusT-Partnerverband ISSS und das Schweizer Informatiksteuerungsorgan des Bundes.

► TeleTrusT-Gremiensitzungen 2017

■ 10.01.2017, Berlin: TeleTrusT-Vorstand
■ 12.01.2017, Berlin: TeleTrusT-AK "Stand der Technik"
■ 30.01.2017, Berlin: TeleTrusT-AG "Smart Grids / Industrial Security"
■ 31.01.2017, Berlin: TeleTrusT-EBCA-AG "Technik"
■ 07.02.2017, Berlin: TeleTrusT-AG "Mobile Security"
■ 28.02.2017, Münster: TeleTrusT-EBCA-Board
■ 02.03.2017 (Telko): T.I.S.P.-Lenkungsgremium
■ 03.03.2017, Berlin: TeleTrusT-AK "Stand der Technik"
■ 03.04.2017 (Telko): TeleTrusT-AG "Blockchain"
■ 11.04.2017 (Telko): TeleTrusT-T.I.S.P.-Lenkungsgremium
■ 27.04.2017, Berlin: TeleTrusT-EBCA-AG "Technik"
■ 02.05.2017 (Telko): TeleTrusT-AK "Stand der Technik"
■ 03.05.2017, Berlin: TeleTrusT-AG "Blockchain"
■ 09.05.2017, Frankfurt/Main: TeleTrusT-EBCA-Board
■ 29.05.2017, Berlin: TeleTrusT-AG "Smart Grids/Industrial Security"
■ 01.06.2017, Berlin: TeleTrusT/ADM-AG "IT-Sicherheit in der Marktforschung"
■ 02.06.2017 (Telko): TeleTrusT-AK "Stand der Technik"
■ 02.06.2017 (Telko): TeleTrusT-AK "SICCT"
■ 13.06.2017 (Telko): TeleTrusT-AK "Smart Grids/Industrial Security"
■ 29.06.2017, Essen: TeleTrusT-Vorstand
■ 31.08.2017, Berlin: TeleTrusT-Engagement in ECSO
■ 07.09.2017, Paderborn: TeleTrusT-EBCA-AG "Technik"
■ 12.09.2017, Berlin: TeleTrusT-AG "RSA (2018)"
■ 21.09.2017, Berlin: TeleTrusT-EBCA-Board
■ 06.10.2017, Berlin: TeleTrusT-Vorstandssitzung
■ 21.11.2017, Berlin: TeleTrusT-AG "RSA (2018)"
■ 30.11.2017, Berlin: TeleTrusT-Vorstandssitzung
■ 01.12.2017, Berlin: TeleTrusT-Mitgliederversammlung
■ 01.12.2017, Berlin: TeleTrusT-Vorstandssitzung
■ 12.12.2017, Berlin: TeleTrusT-AG "Biometrie"

► TeleTrusT-Eigenveranstaltungen 2017

■ 11./12.01.2017, Karlsruhe (secorvo): Interner Workshop der T.P.S.S.E-Schulungsanbieter
www.teletrust.de/veranstaltungen/tutorials-workshops/tpsse-workshop/

■ 19.01.2017, Berlin (TeleTrusT): Interner Workshop der TeleTrusT-AG "SICCT"
www.teletrust.de/veranstaltungen/tutorials-workshops/interner-workshop-der-teletrust-ag-sicct/
■ 12.05.2017, München: TeleTrusT-Regionalstelle München (itWatch)
■ 31.05.2017, Berlin: TeleTrusT-Informationstag "IT-Sicherheit in Arztpraxen"
■ 08.06.2017, Hamburg: TeleTrusT-Regionalstelle Hamburg (WMC)
■ 21.06.2017, Berlin: TeleTrusT-EBCA-"PKI-Stammtisch"
■ 22.06.2017, Berlin (TeleTrusT): PKI-Workshop der TeleTrusT-EBCA
www.teletrust.de/veranstaltungen/tutorials-workshops/ebca-pki-2017/
■ 29./30.06.2017, Essen (secunet): TeleTrusT-interner Workshop 2017
www.teletrust.de/veranstaltungen/tutorials-workshops/teletrust-iws-2017/
■ 13.07.2017, Frankfurt/Main: TeleTrusT-Workshop "Blockchain"
www.teletrust.de/veranstaltungen/blockchain/
■ 20.09.2017, Berlin: TeleTrusT/VOI-Informationstag "Elektronische Signatur"
www.teletrust.de/veranstaltungen/signaturtag/infotag-elektronische-signatur-2017
■ 05.10.2017, Crailsheim: TeleTrusT + Cluster Automation & Mechatronik: Workshop zu "Industrial Security"
www.teletrust.de/veranstaltungen/tutorials-workshops/industrial-security-2017/
■ 10.10.2017, Nürnberg: (auf it-sa 2017)
- TeleTrusT-Auditorium "Blockchain - Anwendungsszenarien"
- TeleTrusT-Vortrag: "Der neue Maßstab der IT Security - Update zum Stand der Technik"
- TeleTrusT + Hexatrust: "IT Security in Germany and France - Opportunities for co-operation" www.teletrust.de/veranstaltungen/it-sa/it-sa-2017
■ 07.11.2017, Berlin: TeleTrusT/BvD - IT-Sicherheitsrechtstag 2017 / Umsetzung von Datenschutz-Grundverordnung und IT-Sicherheitsgesetz in der Praxis
www.teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dgsvo/2017/
■ 14./15.11.2017, Berlin: TeleTrusT Information Security Professional (T.I.S.P.) "Community Meeting" 2017
www.teletrust.de/tisp/tisp-community-meeting/2017/
■ 01.12.2017, Berlin: TeleTrusT-Mitgliederversammlung

4 Neue Kooperationen

► Partnerschaft zwischen TeleTrusT und Kuratorium Sicheres Österreich

TeleTrusT und das Kuratorium Sicheres Österreich (KSÖ) sind übereingekommen, als Organisationen partnerschaftlich zu kooperieren.

Das KSÖ Kuratorium Sicheres Österreich ist ein gemeinnütziger unabhängiger Verein, der sich als nationale Vernetzungs-und Informationsplattform für Themen der Inneren Sicherheit zum Ziel gesetzt hat, Österreich sicherer zu machen. Das Kuratorium fungiert als Schnittstelle zwischen Wirtschaft, Forschung, Behörden und Gesellschaft und trägt als Kompetenznetzwerk dazu bei, die relevanten Akteure zusammenzuführen um gemeinsam an diesem Ziel zu arbeiten. Die Kernkompetenzen des KSÖ liegen vor allem in den Bereichen Cybersecurity, Gewaltprävention und Awareness, umfassen jedoch insgesamt eine Vielzahl weiterer wesentlicher Aspekte rund um das Thema Sicherheit. Der Verein setzt sich aus namhaften, für die Sicherheit Österreichs verantwortlichen Unternehmen, Funktionären und Partnern zusammen.

www.kuratorium-sicheres-oesterreich.at/

Die Partnerschaft mit dem KSÖ ergänzt das bereits umfangreiche TeleTrusT-Netzwerk in Österreich.

www.teletrust.de/markterkundung/oesterreich/

► Verbandspolitische Kooperation mit französischem Partnerverband Hexatrust

Hexatrust ist ein TeleTrusT ähnlicher Verband von IT-Sicherheitsunternehmen in Frankreich. Anlässlich einer Erörterungsrunde auf Vorstandsebene, die eine Fortsetzung früherer Gespräche war, wurde die Partnerschaft beider Verbände formell etabliert. Die it-sa 2017 bot dann bereits Gelegenheit für einen Gemeinschafts-Workshop.

► Neue Partnerschaften der TeleTrusT European Bridge CA: SecCommerce und intarsys

Ausweitung des Vertrauensnetzwerkes auf Prozesse rund um die Signatur und Signaturprüfung von digitalen Dokumenten

Die TeleTrusT European Bridge CA kooperiert seit Anfang 2017 mit den Herstellern SecCommerce und intarsys in den Bereichen Signierung, Signaturvalidierung, Verschlüsselung und Entschlüsselung von digitalen Dokumenten. Dadurch ist es Anwendern möglich, durch Mitarbeiter der Organisationen des Vertrauensnetzwerkes Dokumente digital unterschreiben zu lassen und diese auf der Gegenseite erfolgreich auf Gültigkeit zu prüfen.

Die Kooperation mit SecCommerce bietet zudem die technische Grundlage dafür, als Teilnehmer der EBCA an öffentlichen Ausschreibungen teilzunehmen, ohne zusätzliche Zertifikate nutzen zu müssen. Im Rahmen der intarsys-Kooperation erfolgte die Integration in ein E-Mail-Gateway, sodass auch der Austausch signierter und verschlüsselter E-Mails reibungslos umgesetzt werden kann.

www.ebca.de/

► TeleTrusT European Bridge CA: Kooperationsverträge mit PrivaSphere (CH) und T-Systems International

TeleTrusT hat weitere Kooperationen im Rahmen des PKI-Verbunds "TeleTrusT European Bridge CA" (EBCA) vereinbart: mit der PrivaSphere AG (CH) und mit der T-Systems International GmbH (DE). Ziel ist die fortschreitende Verbreitung der EBCA.

PrivaSphere AG
PrivaSphere ist eine Schweizer Plattform für sichere E-Mail und wurde im Oktober 2002 gegründet. Mit PrivaSphere können Unternehmen aller Größen und aus den verschiedensten Branchen spontan sicher via Internet kommunizieren - ohne Installation von Software oder Hardware und ohne in eine eigene E-Mail-Sicherheits-Infrastruktur investieren zu müssen. PrivaSphere Nutzern steht ab sofort der EBCA-Verzeichnisdienst mit allen Teilnehmern transparent und durchgängig zur Verfügung und erleichtert die sichere und effiziente Kommunikation via PrivaSphere an und von Empfängern im europäischen Raum.

T-Systems International GmbH, Trustcenter Solutions
Die Deutsche Telekom AG betreibt seit 1994 ein Trustcenter, das 1998 als erstes bundesweit die Genehmigung zur Ausgabe von Zertifikaten für die digitale Signatur gemäß dem Deutschen Signaturgesetz erhielt.

Durch die EBCA-Kooperationspartner werden ausgewählte E-Mail-Zertifikate mit fortgeschrittenen sowie qualifizierten Signaturen als EBCA-konform anerkannt. Neben den bereits angeschlossenen Partnern erleichtert damit ein weiteres Trustcenter interessierten Organisationen, die Voraussetzungen für die Teilnahme an der EBCA zu erfüllen.

► Neue Partnerschaften der TeleTrusT European Bridge CA: Atos und KDVZ Citkomm

Mit der Atos Information Technology GmbH, einem Anbieter digitaler Zertifizierungsdienste, gewinnt die TeleTrusT EBCA einen weiteren starken Partner für die Fortentwicklung authentischer und verschlüsselter Kommunikation.

Atos wurde gestützt auf eine mit TeleTrusT geschlossene Vereinbarung als vertrauenswürdiger und EBCA-konformer Anbieter von fortgeschrittenen E-Mailzertifikaten gelistet. Neben den schon vorhanden Anbietern können über Atos Zertifikate erworben werden, die von den Mitgliedern der EBCA vollständig akzeptiert werden. Atos leistet damit einen Beitrag für die Etablierung von Vertrauensstellungen zwischen den teilnehmen Unternehmen bzw. deren Certificate Authorities und den damit verbundenen Public-Key-Infrastrukturen.

Eine gleichartige Partnerschaft wurde ebenfalls mit der KDVZ Citkomm geschlossen. Diese stellt als Dienstleister für den EBCA-Teilnehmer BSI (Bundesamt für Sicherheit in der Informationstechnik) einen Teil der Verwaltungs-PKI bereit. Als Körperschaft des öffentlichen Rechts wird KDVZ Citkomm von den drei Kreisen Hochsauerlandkreis, Märkischer Kreis und Kreis Soest sowie von den 41 in diesen Kreisen liegenden Städten und Gemeinden getragen.

► FH Oberösterreich Campus Hagenberg zur TeleTrusT-Regionalstelle ernannt

Der Campus Hagenberg der FH Oberösterreich ist zur "TeleTrusT-Regionalstelle Hagenberg" ernannt worden. Neben TeleTrusT-Regionalstellen in Deutschland, Wien und einem Regionalkontakt in San Francisco bildet Hagenberg damit eine weitere wichtige grenzüberschreitende Verbindung zwischen den in TeleTrusT organisierten IT-Sicherheitskreisen.

► SAMA Partners neue TeleTrusT-Regionalstelle Mannheim
► Detack neue TeleTrusT-Regionalstelle Stuttgart

Die politische und fachliche Diskussion zu aktuellen Fragen der Sicherheit und Vertrauenswürdigkeit von IT-Systemen wird nicht nur auf Bundesebene geführt. Ebenso findet ein Austausch zu diesen Themen auch in den Wirtschaftsregionen und auf verschiedenen politischen Ebenen statt. Über die Etablierung von Regionalstellen, d.h. regionalen Kontakten aus der Mitgliederschaft kann TeleTrusT diesen Austausch vor Ort zwischen lokalen Vertretern der Wirtschaft, öffentlichen Einrichtungen und der Politik fördern und mitgestalten. Als Ansprechpartner und Initiatoren für die Kooperation mit bestehenden regionalen Netzwerken repräsentieren die Regionalstellen den Themenkreis "IT-Sicherheit" bzw. "Sichere und vertrauenswürdige Informationssysteme". Insbesondere der Mittelstand kann auf diesem Weg gut erreicht werden.

TeleTrusT-Mitglied SAMA PARTNERS Business Solutions GmbH hat als neue "TeleTrusT-Regionalstelle Mannheim" die TeleTrusT-Repräsentanz vor Ort übernommen.

In enger Zusammenarbeit mit der Bundesgeschäftsstelle des Verbandes hat TeleTrusT-Mitglied Detack GmbH als Nachfolgerin der CenterTools GmbH die Funktion der "TeleTrusT-Regionalstelle Stuttgart" übernommen.


TeleTrusT
Pioneers in IT security.