Bundesverband IT-Sicherheit e.V.

TeleTrusT
Pioneers in IT security.

Jahresbericht 2018

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:

Bundesverband IT-Sicherheit e.V. (TeleTrusT)
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

Bundesverband IT-Sicherheit e.V. (TeleTrusT)

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung, Beratung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. Durch die breit gefächerte Mitgliederschaft und die Partnerorganisationen verkörpert TeleTrusT den größten Kompetenzverbund für IT-Sicherheit in Deutschland und Europa. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; PKI-Vertrauensverbund), der Expertenzertifikate "TeleTrusT Information Security Professional" (T.I.S.P.) und "TeleTrusT Professional for Secure Software Engineering" (T.P.S.S.E.) sowie des Vertrauenszeichens "IT Security made in Germany". TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI). Hauptsitz des Verbandes ist Berlin.

https://www.teletrust.de

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

Telefon: +49 30 4005 4310

E-Mail: info@teletrust.de

Inhaltsverzeichnis

Vorstand und Geschäftsstelle 2018

► TeleTrusT-Vorstand (bis 30.11.2018)

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

Neuer TeleTrusT-Vorstand ab 30.11.2018 (turnusgemäße Vorstandswahl):

Prof. Dr. Norbert Pohlmann, if(is) - TeleTrusT-Vorsitzender
RA Karsten U. Bartels LL.M., HK2 - Stellvertretender TeleTrusT-Vorsitzender
Axel Deininger, secunet, TeleTrusT-Vorstandsmitglied
Dr. Kim Nguyen, Bundesdruckerei, TeleTrusT-Vorstandsmitglied

► 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

Nicolai Guthmann

Projektkoordinator

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

Vi Linh Tran-Graef

Assistentin

Telefon: +49 30 400 54 307
Telefax: +49 30 400 54 311

Helke Brauch

Projektassistentin

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

Neue Mitarbeiterinnen ab 2018-10:

Michele Decker
Franziska Bock

Verbandsentwicklung 2018

► Mitgliederzahl

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
340										335
330										
320										
310										
300										
290										
280										
270										
260										
250										
240										
230										
220										
210										
200										
190										
180										
170										
160										
150										
140										
130										
120										
115										
110										
105										
100										

► TeleTrusT-Arbeitsgruppen und -Lenkungsgremien 2018

TeleTrusT-Arbeitsgruppen:

"Biometrie"	Leitung: Prof. Dr. Christoph Busch, Fraunhofer IGD Alexander Nouak, Fraunhofer IGD
"Cloud Security"	Leitung: Oliver Dehning, Hornetsecurity
- AK "Mail Security"	Leitung: Peter Hansemann, ICN
"EBCA/Technik"	Leitung: Hendrik Koy, Deutsche Bank
"Forum elektron. 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: Peter Rost, Rohde + Schwarz Cybersecurity
"IT-Sicherheit in der Marktforschung"	Leitung: 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
- NEU: AK "Security by Design"	Leitung: Rolf Blunk, Otaris
"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
"ECSO" (Koordinierungskreis)	Leitung: Gerd Müller, secunet

TeleTrusT-Lenkungsgremien:

Vorstand	Vorsitzender: Prof. Dr. Norbert Pohlmann, if(is) Stellv. Vorsitzender: Dr. Rainer Baumgart, secunet Axel Deininger, secunet, Dr. Kim Nguyen, Bundesdruckerei
"EBCA"	Sprecher: Markus Wichmann, Siemens Henrik Koy, Deutsche Bank, Melanie Wunsch, BSI, Bernhard Hoelcker, E-ON, Stefan Cink, Net at Work, Dr. Holger Mühlbauer, TeleTrusT
"T.I.S.P."	Sprecherin: Birgitte Baardseth, isits NEU: Hans-Peter Möschle, M&H, Hubert Große-Onnebrink, Fraunhofer SIT, Stefan Gora, secorvo, Dr. Holger Mühlbauer, TeleTrusT
"T.P.S.S.E"	NEU: Sprecher: Fabian Ebner, Secorvo Dr. Tobias Koal, Philotech, Dr. Reinhard Schwarz, Fraunhofer IESE, Frank Tenz, SEC, Dr. Holger Mühlbauer, TeleTrusT

► TeleTrusT-Regionalstellen 2018

"Bremen" (repräsentiert durch Otaris)
"Chemnitz" (repräsentiert durch Digitronic)
"Dresden" (repräsentiert durch T-Systems MMS)
"Düsseldorf" (repräsentiert durch Exceet)
"Frankfurt/M." (repräsentiert durch QGroup)
"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)
"Mannheim" (repräsentiert durch Sama Partners)
"München" (repräsentiert durch itWatch)
"Silicon Valley" - US - (repräsentiert durch SEC)
"Stuttgart" (repräsentiert durch Detack)
"Wien" - AT - (repräsentiert durch AIT)

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

BMWi: Beirat Exportinitiative IT-Sicherheitswirtschaft
BMWi: IT-Standardisierungsbeirat
BMWI: Steuerkreis 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
it-sa India: Messebeirat
OMNISECURE: Programmkomitee
RSA Conference: Exhibitor Advisory Council

► TeleTrusT-Verbandsbeziehungen 2018

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)
KSÖ - Kuratorium Sicheres Österreich
NEU: Information Security Network des IT-Clusters der Business Upper Austria (OÖ)

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

► Thema "IT-Sicherheit" im Koalitionsvertrag: TeleTrusT gibt Empfehlungen und sieht gute Ansätze

Cybersicherheit ist ein entscheidender Faktor für die zukünftige internationale Wettbewerbsfähigkeit der deutschen Wirtschaft. So werden Lösungen für Industrie 4.0, intelligente Energienetze, digitalisierte Gesundheitswirtschaft, Smart Home und autonomes Fahren sich nur dann durchsetzen, wenn sie sowohl innovativ als auch vertrauenswürdig sind. Die nächste Bundesregierung muss Cybersicherheit deshalb zu einem Schwerpunkt ihrer Politik machen. Wesentliche Lebensbereiche werden in den kommenden Jahren grundlegend digitalisiert und bieten die Option, von Grund auf sichere Technologien zu entwickeln, ökonomisch zu skalieren und als Standards zu etablieren: die Verkehrssysteme, das Gesundheitswesen, die Energieversorgung, kommunale Infrastrukturen, staatliche Dienstleistungen. Deutschland hat große Chancen, in der Legislaturperiode 2018 bis 2021 und aufbauend auf den bisherigen Ergebnissen der vergangenen Legislaturperiode, bei der Cybersicherheit entscheidend voranzukommen. Die gute wirtschaftliche Lage und die günstige Haushaltslage von Bund und Ländern erlauben erhebliche Investitionen in Cybersicherheit und sichere Digitalisierung.

Die Cybersicherheitspolitik einer neuen Koalition im Bund sollte Schwerpunkte setzen:

■ Ziel sollte es sein, den volkswirtschaftlichen Schaden, der durch mangelnde Informationssicherheit entsteht und der 2017 auf 55 Milliarden Euro beziffert wird, bis zum Ende der Legislaturperiode mindestens zu halbieren. Hierzu fordert TeleTrusT 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. Mit der geforderten Investition würde der digitale Standort Deutschland nachhaltig attraktiver werden - auch für ausländische Investoren. Gleichzeitig würde die neue Bundesregierung die Chance nutzen, die eigene IT-Sicherheitswirtschaft zu stärken und europäische und internationale Kooperationsprojekte aufzubauen.

■ Einrichtung eines Runden Tisches zur Erarbeitung und Nachhaltung einer Cybersicherheitsstrategie mit konkreten, messbaren Zielen zur Erhöhung der Informationssicherheit, gemeinsam mit Bund, Ländern, Wirtschaft und Wissenschaft

■ Personelle Stärkung des Bundesamtes für Sicherheit in der Informationstechnik (BSI)
Zulassungs- und Zertifizierungsverfahren müssen beschleunigt werden, um so den Anwendern nachweislich sichere digitale Prozesse, Produkte und Lösungen schneller zur Verfügung stellen zu können. Erhöhung des BSI-Budgets für die Entwicklung neuer gesamtwirtschaftlicher und staatlich erforderlicher Basis-Sicherheitsprodukte

■ Neue Anreizsysteme, mit denen Behörden und Unternehmen die vom BSI empfohlenen, dem Stand der Technik entsprechenden IT-Sicherheitsmaßnahmen aufbauen können und Etablierung breiter Programme für Wirtschaft und Behörden, um die vorhandenen Cybersicherheits-Lösungen der deutschen IT-Sicherheitswirtschaft besser bekannt zu machen

■ Informationssicherheit wird nicht ohne einen Paradigmenwechsel in der Digitalisierung gelingen. Daher sind beweisbar sichere Technologien ("Security by design") mittels Forschung und Beschaffung weiter zu fördern. IT-Hersteller und -Diensteanbieter sollen für Datenschutz- und IT-Sicherheitsmängel ihrer Produkte haften.

■ 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.

■ Förderung der Entwicklung vertrauenswürdiger IT- und Netz-Infrastruktur sowie sicherer Soft- und Hardware und sicherer Cloud-Technologie
Ferner sollen Fähigkeiten zur Bekämpfung von staatlichen und nichtstaatlichen Bedrohungen im Cyberraum geschaffen werden. Hierzu sollen auch Anbieter und Technologie-Startups zur Schaffung nationaler Schlüsselkompetenzen gezielt gefördert werden. Förderung von Open-Source Technologien im Cybersicherheitsbereich.

■ Die weitere Förderung von Kompetenz auf dem Gebiet der Kryptosystemtechnologie, die kurzfristig von Staat und Industrie genutzt werden kann, ist essentiell. Zusätzlich dazu soll das Bundesministerium für Wirtschaft, Energie und Technologie im Bereich IT-Sicherheit und Kryptotechnologie einen neuen wirtschaftspolitischen Strang zur Förderung dieser Bereiche anlegen. 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.

TeleTrusT begrüßt einzelne Inhalte des Koalitionsvertragsentwurfes, soweit sie sich auf den Themenkreis IT-Sicherheit beziehen. Insbesondere greift der Vertragsentwurf die TeleTrusT-Forderung nach Entwicklung einer übergreifenden Cybersicherheitsstrategie auf ("Cyberpakt"). Gleichwohl bleiben Inkonsistenzen.

TeleTrusT begrüßt ausdrücklich die Aussagen des Koalitionsvertrages zu Innovation, digitaler Souveränität und Interdisziplinarität sowie zur Stärkung der IT-Sicherheitsforschung insbesondere auf den Gebieten Blockchain und Quantencomputing (Kapitel IV "Offensive für Bildung, Forschung und Digitalisierung"; Unterkapitel "Digitalisierung").

Begrüßenswert ist ebenso die Absicht, das Produktsicherheitsrecht zu novellieren und für verbrauchernahe Produkte die IT-Sicherheit u.a. durch die Einführung einer "gewährleistungsähnlichen Herstellerhaftung" zu erhöhen. Ferner wollen Union und SPD die Verbreitung sicherer Produkte und das Prinzip "Security by Design" fördern. Letzteres bedeutet, dass bei der Entwicklung von Hard- und Software schon von Beginn an darauf geachtet wird, dass Systeme frei von Schwachstellen und so gegen Cybertattacken geschützt sind und nicht erst am Ende der Entwicklungskette. Das entspricht früheren TeleTrusT-Forderungen. Zudem soll ein Gütesiegel für IT-Sicherheit auf Produkten mehr Transparenz für Verbraucher schaffen.

Positiv zu bewerten ist das Vorhaben, die Rolle des Bundesamtes für die Sicherheit in der Informationstechnik im Verbraucherschutz zu stärken und Unternehmen zur Offenlegung und zur Beseitigung von Sicherheitslücken zu verpflichten. Zu begrüßen ist auch die Zielsetzung, "Ende-zu-Ende-Verschlüsselung für jedermann verfügbar" zu machen und es Bürgerinnen und Bürgern zu ermöglichen, "verschlüsselt mit der Verwaltung über gängige Standards zu kommunizieren". Dieser sinnvolle Ansatz wird allerdings nicht konsequent durchgehalten und teils konterkariert, denn weder ist ein Verbot für staatliche Stellen, Zero Day Exploits anzukaufen, noch eine ausdrückliche Verpflichtung dieser Stellen, derartige Sicherheitslücken bekanntzumachen, beabsichtigt. Statt dessen heißt es: "Es darf für die Befugnisse der Polizei zu Eingriffen in das Fernmeldegeheimnis zum Schutz der Bevölkerung keinen Unterschied machen, ob die Nutzer sich zur Kommunikation der klassischen Telefonie oder klassischer SMS bedienen oder ob sie auf internetbasierte Messenger-Dienste ausweichen." Dies kann nur so verstanden werden, dass die Sicherheitsbehörden entweder die Möglichkeit haben sollen, auch verschlüsselte Kommunikation mitzulesen oder diese Kommunikation unter Ausnutzung von Sicherheitslücken mit Hilfe der Quellen-TKÜ in unverschlüsselter Form mitzulesen. Mit der Zielsetzung, die IT-Sicherheit insgesamt zu verbessern, passt keine der beiden Varianten zusammen.

► Was ist "Stand der Technik" nach IT-Sicherheitsgesetz und DSGVO?

TeleTrusT veröffentlicht revidierte und erweiterte Handreichung zum Stand der Technik in der IT-Sicherheit

Mit dem "Gesetz zur Erhöhung der Sicherheit informationstechnischer Systeme" (IT-Sicherheitsgesetz bzw. ITSiG) verfolgt der Gesetzgeber das Ziel, Defizite in der IT-Sicherheit abzubauen. Daneben gilt seit dem 25.05.2018 die EU-Datenschutz-Grundverordnung (DSGVO) mit ihren hohen Anforderungen an die technischen und organisatorischen Maßnahmen. Beide Rechtsquellen fordern die Orientierung der IT-Si-

cherheit am Stand der Technik, lassen aber unbeantwortet, was im Detail darunter zu verstehen ist. TeleTrusT hat seine Handreichung zum Stand der Technik überarbeitet und im Lichte neuer Erkenntnisse erweitert.

Täglich zeigen Meldungen zu Sicherheitsvorfällen in Unternehmen und Behörden, dass dringender Handlungsbedarf zur Verbesserung der IT-Sicherheit besteht. Artikel 32 DSGVO regelt zur "Sicherheit der Verarbeitung", dass "unter Berücksichtigung des Standes der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technische und organisatorische Maßnahmen zu treffen sind." Damit soll ein dem Risiko angemessenes Schutzniveau gewährleistet werden, z.B. durch Maßnahmen wie Verschlüsselung.

Sowohl der nationale als auch der europäische Gesetzgeber enthalten sich jedoch konkreter, detaillierter technischer Anforderungen und Bewertungskriterien für die sicherheitsrelevanten technischen und organisatorischen Maßnahmen. Den Gesetzesadressaten werden auch keinerlei methodische Ansätze geliefert. Diese Ausgestaltung, zumal in einem dynamischen Marktumfeld, muss den Fachkreisen überlassen bleiben.

TeleTrusT flankiert und ergänzt die Rechtslage mit der fachlichen Kompetenz der organisierten IT-Sicherheitswirtschaft in Deutschland. Eine Expertengruppe hat die bestehende "TeleTrusT-Handreichung zum Stand der Technik" überarbeitet und ergänzt. Das Dokument gibt konkrete Hinweise und Handlungsempfehlungen.

https://www.teletrust.de/arbeitsgremien/recht/stand-der-technik/

Die Handreichung versteht sich als Ausgangspunkt bei der Ermittlung von gesetzlichen IT-Sicherheitsmaßnahmen. Sie ersetzt nicht eine technische, organisatorische oder rechtliche Beratung bzw. Bewertung im Einzelfall.

► TeleTrusT: Cyber-Sicherheit muss politische Priorität haben

TeleTrusT fordert Einhaltung des Koalitionsvertrages: Stellenbesetzungszusagen für das BSI, Ausbau zur nationalen Cyber-Sicherheitsbehörde, IT-Sicherheit als notwendiger Rahmen für die Digitalisierung

Informationstechnik ist Motor und Basis der modernen, globalen Informations- und Wissensgesellschaft. Gleichzeitig ist offensichtlich, dass die derzeitigen IT-Architekturen bei Endgeräten, Servern und Netzkomponenten nicht sicher genug konzipiert sind, um den Fähigkeiten intelligenter Hacker standzuhalten. Vor diesem Hintergrund ist nicht nachvollziehbar, dass im aktuellen Haushalt 2018 des Bundesministeriums des Innern, für Bau und Heimat (BMI) keine neuen Stellen für den Ausbau des Bundesamtes für Sicherheit in der Informationstechnik (BSI) zur nationalen Cyber-Sicherheitsbehörde eingeplant wurden, wie noch im Koalitionsvertrag angekündigt.

Täglich kann den Medien entnommen werden, wie kriminelle Hacker unzureichende Softwarequalität für erfolgreiche Angriffe nutzen, Malware installieren, Passwörter und Identitäten stehlen und Endgeräte ausspionieren. Aktuelle Beispiele sind der Angriff auf den Bundestag und das Auswärtige Amt, Hardwareschwachstellen in Mikroprozessoren, schlecht implementierte E-Mail-Clients, Manipulation von Wahlen. Es ist ein politischer Widerspruch, einerseits auf fortschreitende Digitalisierung zu setzen und andererseits die notwendigen Cyber-Sicherheitsherausforderungen zu vernachlässigen. Die Digitalisierung bis hin zum Ausbau Künstlicher Intelligenz muss mit IT-Sicherheitsmaßnahmen als notwendiger Kehrseite begleitet werden, damit sie nachhaltig gelingen kann.

TeleTrusT erinnert daran, die Zusagen aus dem Koalitionsvertrag einzuhalten, einen deutlich stärkeren Schwerpunkt auf die Stärkung der IT-Sicherheit zu legen und die Einrichtung eines nationalen Paktes für Cyber-Sicherheit sowie den Ausbau des BSI zur nationalen Cyber-Sicherheitsbehörde, einschließlich eines Zuwachses um mindestens 200 Stellen, umzusetzen.

Das IT-Sicherheitsgesetz, die technisch-organisatorischen Maßnahmen aus der Datenschutz-Grundverordnung, Hardwaresicherheit und Sicherheit bei Industrie 4.0 sind dringende Herausforderungen, denen nur mit angemessenen Ressourcen entsprochen werden kann.

► TeleTrusT: E-Mail-Verschlüsselung bleibt sicher - Angriff auf PGP- und S/MIME-Verschlüsselung nutzt Schwachstellen in E-Mail-Clients

Am 14.05.2018 veröffentlichte ein Team aus Sicherheitsforschern der Fachhochschule Münster, der Ruhr Universität Bochum und der Universität Leuven (Belgien) einen Bericht, der die Sicherheit der Verschlüsselungsstandards PGP und S/MIME in Frage stellt und damit weltweites Aufsehen erregte. Die aufgedeckten Sicherheitslücken (CVE-2017-17688 und CVE-2017-17689) betreffen jedoch nicht die Protokolle selbst, sondern nutzen eine bereits länger bekannte Schwachstelle in E-Mail-Clients, um verschlüsselte E-Mails zu entschlüsseln und dem Angreifer zuzustellen. Die Angriffe sind technisch komplex und benötigen mehrere Schritte zur erfolgreichen Umsetzung.

Erste Voraussetzung für einen erfolgreichen Angriff: Die E-Mail muss bereits in verschlüsselter Form beim Angreifer vorliegen. Hierfür muss er die E-Mails auf dem Transportweg per "Man-in-the-Middle"-Attacke abfangen oder einen Mailserver kompromittiert haben.

Anschließend könnten die Angreifer laut den Autoren des Papers zwei sich ähnelnde Angriffsmethoden anwenden, um E-Mails mit vorhandener PGP- oder S/MIME-Verschlüsselung zu entschlüsseln. Der erste Angriff ist recht simpel auszuführen, dafür aber auf bestimmte Mail-Clients (Apple-Mail, iOS-Mail, Mozilla Thunderbird) und ggf. dort installierte Plugins von Drittanbietern beschränkt. Die zweite Möglichkeit, um PGP- oder S/MIME-verschlüsselte E-Mails auszulesen, besteht aus einer schon länger bekannten Methode zum Extrahieren von Plaintext in Blöcken verschlüsselter Nachrichten. Bei beiden Arten werden die abgefangenen verschlüsselten E-Mails manipuliert. Wichtig bei diesen beiden Angriffsmethoden ist, dass die Verschlüsselungsmethoden S/MIME und PGP selbst nicht gebrochen werden; vielmehr nutzen sie Schwachstellen in E-Mail-Clients für HTML-Mails aus, um die Verschlüsselungstechniken zu umgehen.

Auch das Bundesamt für Sicherheit in der Informationstechnik weist darauf hin, dass PGP und S/MIME weiterhin sicher eingesetzt werden können, wenn sie korrekt implementiert und sicher konfiguriert sind.

► TeleTrusT-Kommentierung zu BNetzA-Regelungen betreffend die Nutzung von Videoident-Verfahren für QES

TeleTrusT hat im Namen konsultierter Fachkreise die Regelungen aus der BNetzA-Mitteilung Nr. 208-2018 (Amtsblatt) kommentiert. Hauptpunkt der Kommentierung seitens TeleTrusT ist die Fragestellung, inwieweit die Verfügung konform zum Erwägungsgrund 54 der EU-Verordnung Nr. 910/2014 ist. Es werden in dieser Verfügung Festlegungen für Qualifizierte Zertifikate getroffen, die über die EU-Verordnung hinausgehen. Dadurch würden für in Deutschland ansässige Vertrauensdiensteanbieter (VDA) strengere Anforderungen als für die VDA in anderen EU-Staaten gelten, was die Entwicklung des Europäischen Binnenmarktes behindern könnte.

Die TeleTrusT-Kommentierung ist hier abrufbar: https://www.teletrust.de/publikationen/stellungnahmen/ (12.07.2018)

► Bewertung der Stellungnahme des IMCO-Ausschusses des EP zum Entwurf einer EU-Cybersecurity-Verordnung

Am 22.05.2018 hat der Ausschuss für den Binnenmarkt und Verbraucherschutz (IMCO) des Europaparlaments seine Stellungnahme zu dem "Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die "EU-Cybersicherheitsagentur" (ENISA) und zur Aufhebung der Verordnung (EU) Nr. 526/2013 sowie über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik ("Rechtsakt zur Cybersicherheit")" - bekannt auch als "Cybersecurity-Verordnung" - veröffentlicht.

Einer der Hauptbestandteile des Entwurfes der EU Cybersecurity-Verordnung ist die so genannte "Konformitätsbewertung", innerhalb derer festzustellen ist, ob IKT-Produkte oder -Dienste die an die Cybersicherheitsmerkmale anzulegenden Anforderungen erfüllen. Da eine Zertifizierung von IKT-Produkten und -Diensten nicht zwingend aussagt, dass diese tatsächlich und in jedem Falle sämtliche an die Cybersicherheit anzulegenden Kriterien erfüllen, fordert das IMCO-Committee explizit und weitergehend als der Verord-

nungsentwurf, dass Verbraucher über die Restrisiken der Zertifizierung aufzuklären sind, indem unter anderem darauf hingewiesen wird, dass die entsprechenden Produkte und Dienste nur auf die Übereinstimmung mit beispielsweise in technischen Normen und Standards festgelegten Anforderungen an die Cybersicherheit hin überprüft wurden.

Transparenz, Beteiligung und angemessene Verfahrensvorgaben sind von hoher Bedeutung für die Einrichtung und das Funktionieren eines vertrauenswürdigen und effektiven europäischen Cyber-Sicherheitsrahmens. Eng verbunden mit der Definition von Mindestsicherheitsstandards für IT-Produkte ist das Ziel, die Prinzipien von "Security by Design" sowie von "Privacy by Design" konsequent umzusetzen und umfassend in Produkte und Dienste zu integrieren. Hierzu soll das europäische Zertifizierungssystem für Cybersicherheit laut der Auffassung des IMCO-Ausschusses so ausgestaltet werden, dass alle hierdurch betroffenen Akteure die IT-Sicherheitsanforderungen in allen Phasen des Produkt- oder Dienstlebenszyklus umsetzen. Eine umfassende Auseinandersetzung mit europaweiten Fragen der Cybersicherheit setzt darüber hinaus die Bestimmung von Anforderungen im Umgang mit Backdoors in IKT-Produkten und -Diensten voraus.

Der IMCO-Ausschuss hat im Vergleich zum ursprünglichen Kommissionsentwurf zahlreiche Änderungsvorschläge der EU Cybersecurity-Verordnung hervorgebracht, worunter sich auch verschiedene interessante und neuartige Ansätze finden.

Auf Bitten von TeleTrusT hat Dr. Dennis Kipker (Universität Bremen; TeleTrusT-Mitglied) die IMCO-Stellungnahme einer Betrachtung unterzogen: https://www.teletrust.de/publikationen/stellungnahmen/.

► 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.

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.

► 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.

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

Im Rahmen eines Stellungnahmeverfahrens 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.

► TeleTrusT-Stellungnahme zur Änderung des Onlinezugangsgesetzes und der Abgabenordnung

Mit Fristsetzung 22.11.2018 hatte das Bundesministerium des Innern, für Bau und Heimat, Referat DG II 3, zur Stellungnahme zu geplanten Änderungen des Onlinezugangsgesetzes und der Abgabenordnung aufgerufen. TeleTrusT kommentierte fristgerecht unter Einbeziehung der AG "Forum elektronische Vertrauensdienste". Die Kommentierung bezog sich auf den Nachweis der Identität des Nutzers eines Nutzerkontos auf unterschiedlichen Vertrauensniveaus in allen zulässigen Identifikationsverfahren.

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

■ 16.01.2018, Berlin
Mitwirkung bei "Zum staatlichen Umgang mit Verschlüsselung": Publikationsvorstellung und Diskussion, Heinrich-Böll-Stiftung/Global Public Policy Institute

■ 31.01.2018, Berlin, BMWi
Mitwirkung an einer Besprechung zur deutsch-indischen Zusammenarbeit bei Digitalthemen
- Multistakeholder-Ansatz der Internet-Verwaltung
- Informationsaustausch über digitale Kernaktivitäten
- Zusammenarbeit von öffentlichen und privaten Akteuren auf dem Gebiet der IKT
- Förderung der Zusammenarbeit von Unternehmen und Forschungseinrichtungen
- Förderung von Fachkräften für Bildung und Ausbildung im IKT-Sektor; Berufsbildung
- Förderung der Zusammenarbeit auf dem Gebiet der Normung und Konformitätsbewertung
- Regulierungspolitik, Entwicklung digitaler Produktions- und Dienstleistungsindustrien
- Aktivitäten in internationalen Foren, Teilnahme an internationalen Veranstaltungen
- [TeleTrusT ist Partner der it-sa India in Mumbai; s.u.]

■ 02.2018, Berlin
"Digitalminister/in gesucht": TeleTrusT unterstützte die Initiative des Bundesverbandes Deutsche Start-ups e.V., mit der die Vorsitzenden von CDU, CSU und SPD aufgefordert werden, die Digitalisierung mit einer festen Verantwortlichkeit innerhalb der neuen Bundesregierung organisatorisch zu verankern und eine/n Digitalminister/in zu ernennen.

■ 2018-02, Berlin/Bonn, BNetzA
Im Rahmen eines anhängigen Konsultationsverfahrens der Bundesnetzagentur zum Entwurf eines IT-Sicherheitskatalogs für Energieanlagen nach § 11 Absatz 1b Energiewirtschaftsgesetz hat TeleTrusT eine Kommentierung abgegeben.

■ 26.02.2018, Berlin, BMWi
Präsentation der Ergebnisse unserer Studie "Einsatz von elektronischer Verschlüsselung - Hemmnisse in der Wirtschaft“

■ 26.02.2018, Berlin Capital Club
TeleTrusT-Neujahrsempfang

Der TeleTrusT-Neujahrsempfang führte Verbandsmitglieder bzw. Vertreter aus Industrie, Politik, Medien und Forschung zusammen. Saskia Esken (MdB; SPD) kennzeichnete in ihrer Gastrede das Thema IT-Sicherheit als wichtigen Schwerpunkt der kommenden Legislaturperiode, während gleichzeitig der "Bundestrojaner" ein hochproblematischer Eingriff sei.

■ 05.03.2018, Berlin, BMWi
Mitwirkung am Workshop "IT-Sicherheit in KMU"

■ 12.03.2018, Berlin, BSI-Forschungsprojekt "IT-Sicherheitsregulierung", München
Mitwirkung am Expertenworkshop

■ 23.03.2018, Berlin, BSI
Teilnahme am BSI-Arbeitsfrühstück "10 Jahre Grundrecht auf Vertraulichkeit und Integrität informationstechnischer Systeme"

■ 10.04.2018, Berlin, BMWi
Mitwirkung am Erörterungstreffen zum "Deutsch-Chinesischen Cyber-Konsultationsmechanismus"

■ 13.04.2018, Berlin, Bundesnetzagentur
Beteiligung an der AG "Intelligente Netze und Zähler der Plattform Energienetze"

■ 08.05.2018, Berlin, BMWi/DIN/SBS
"Geschäftschancen in Indien für zivile Sicherheitstechnologien und -dienstleistungen mit Fokus auf IT-Sicherheitstechnologien"

Mitwirkung an einer Informationsveranstaltung der Exportinitiative "Zivile Sicherheitstechnologien" (Angesprochen wurden im Rahmen dieser Veranstaltung unter anderem die nicht akzeptablen langen BAFA-Genehmigungsverfahren.)

■ 29.08.2018, Berlin, Auswärtiges Amt
Wirtschaftstag der Botschafterkonferenz im Auswärtigen Amt, Berlin

■ 06.09.2018, Australische Botschaft
Teilnahme am Luncheon der Australischen Botschafterin in Kooperation mit Standards Australia zum Thema "Blockchain and Distributed Ledger Technologies"

■ 2018-10/11
"Mindeststandards für staatliches Hacking"/"A Framework for Government Hacking in Criminal Investigations"

Unterstützung einer Publikation der "Stiftung Neue Verantwortung" (Publikation im Rahmen des Cybersicherheitsexperten-Netzwerks "Transatlantic Cyber Forum")
https://www.stiftung-nv.de/sites/default/files/framework_for_government_hacking_in_criminal_investigations.pdf

■ 2018-11
"Der Datenschutzbeauftragte: Wettbewerbsvorteil für deutsche Unternehmen und Schutz von Verbraucherrechten - Positionspapier zur Benennungspflicht eines betrieblichen Datenschutzbeauftragten in kleinen und mittelständischen Unternehmen"

Unterstützung einer Initiative des BVD - Berufsverband der Datenschutzbeauftragten e.V. (TeleTrusT-Partnerverband)

■ 20.11.2018, Berlin, BMWi
Mitwirkung im Beirat für Standardisierung in der IKT

■ 03./04.12.2018, Nürnberg
Mitwirkung am "Nationalen Digital-Gipfel" 2019

■ 2018-12, BMWi
Beteiligung an der Zielländer-Präferenzumfrage für das KMU-Markterschließungsprogramm 2019

2 Ausgewählte Themen

► TeleTrusT jetzt reguläres Mitglied im DIN Deutsches Institut für Normung e.V.

TeleTrusT ist nunmehr reguläres Mitglied im DIN Deutsches Institut für Normung e.V. Bereits bisher war bzw. ist TeleTrusT 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 Co-ordination Group. TeleTrusT unterstützt die jährliche "KITS-Konferenz" des DIN sowie anlassbezogen Veranstaltungen der DIN-Akademie und des Beuth-Verlages.

Darüber hinaus ist TeleTrusT ETSI-Mitglied und bei ISO engagiert.

https://www.teletrust.de/standardisierung

► TeleTrusT übernimmt stellvertretenden Vorsitz des deutschsprachigen Begleitgremiums zu ISO/TC 225 "Market, opinion and social research"

TeleTrusT hat per Gremiumsbeschluss auf einer Sitzung am 15.01.2018 in Wien den stellvertretenden Vorsitz des deutschsprachigen Begleitgremiums zu ISO/TC 225 "Market, opinion and social research" übernommen. ISO/TC 225 erarbeitet zertifizierungsfähige internationale Normen für die Markt-, Meinungs- und Sozialforschung einschließlich Webanalysen. TeleTrusT vertritt in der Fachdiskussion das Thema IT-Sicherheit. In dem deutschsprachigen Spiegelgremium in Trägerschaft von Austrian Standards stimmen Marktforschungsverbände aus Deutschland, Österreich und der Schweiz ihre Positionen ab. Den Vorsitz hat Robert Sobotka, Präsident des Verbandes Österreichischer Marktforscher (VMÖ).

► 1.000ster Absolvent des T.I.S.P.-Programms

Expertenzertifikat "TeleTrusT Information Security Professional" ist gefragt

Mit dem Expertenzertifikat "TeleTrusT Information Security Professional" (T.I.S.P.) weisen Fachleute aus Unternehmen und Institutionen fortgeschrittene Kenntnisse auf dem Gebiet IT-Sicherheit nach. Mit Kai Riecke, CTO Hubert Burda Media, Vorstandsbereich Medienmarken National, hat der 1.000ste IT-Sicherheitsexperte das T.I.S.P.-Programm erfolgreich absolviert.

Mit einer erfolgreich abgelegten Prüfung zum T.I.S.P. belegt ein Kandidat seine umfassenden und ganzheitlichen Kenntnisse und Fähigkeiten im IT-Sicherheitsumfeld auf operativer, taktischer und strategischer Ebene. Der Schwerpunkt der Prüfung liegt auf dem Test eines ganzheitlich vorhandenen Denkansatzes für das IT-Sicherheitsmanagement unter Einbezug der spezifischen europäisch geprägten Sicherheitskultur und der einschlägigen gesetzlichen Normen und Standards. Eine erfolgreiche Ausbildung zum T.I.S.P. setzt ausreichende theoretische und praktische Kenntnisse und Fertigkeiten auf dem Gebiet des IT-Sicherheitsmanagements sowie der Techniken, Technologien und Produkte voraus. Das Zertifizierungsprogramm umfasst eine mehrtägige Schulung, an die sich eine intensive Prüfung anschließt. Das Zertifikat hat eine Gültigkeit von drei Jahren und kann durch Rezertifizierung verlängert werden. Zertifikate wie der T.I.S.P. sind nachgefragtes Indiz für hochspezialisiertes Fachwissen und helfen bei der beruflichen Weiterentwicklung, da sie Arbeitgebern als Beleg für persönliche Qualifikation dienen, die dem Unternehmen zugute kommt.

https://www.teletrust.de/tisp/

► Europäisches Markenamt genehmigt Eintragung der TeleTrusT-Marke "T.P.S.S.E."

Das EU-Markenamt hat die Eintragung der TeleTrusT-Marke "T.P.S.S.E." in den angemeldeten Waren- und Dienstleistungsgruppen genehmigt. Ein zuletzt anhängiger Einspruch aus Spanien wurde von dort zurückgezogen.

Schwerpunkt der T.P.S.S.E.-Zertifizierung ist die Expertise, wie und wo Softwarenentwicklung mit Sicherheitsaspekten sinnvoll ergänzt werden kann. Mit Absolvierung einer Schulung und der unabhängigen Prüfung zum T.P.S.S.E. wird als Qualifikationsnachweis ein anerkanntes Expertenzertifikat erworben.

https://www.teletrust.de/tpsse/

► Wirtschaftsminister Altmaier: Grußwort für die TeleTrusT-Initiative "IT Security made in Germany"

TeleTrusT begrüßt, dass Bundeswirtschaftsminister Altmaier die Tradition der Grußworte für die TeleTrusT-Initiative "IT Security made in Germany" fortsetzt und ein Grußwort übermittelt hat:

https://www.teletrust.de/itsmig/grusswort/

Das BMWi unterstreicht damit seine kontinuierliche Unterstützung.

► Neuer TeleTrusT-Arbeitskreis "Security by Design" konstituiert

Wie auf dem TeleTrusT-internen Workshop 2018 beschlossen, konstituierte sich auf einer Sitzung am 07.09.2018 in Berlin der neue TeleTrusT-AK "Security by Design". Der AK ist eine Untergliederung der TeleTrusT-AG "Recht". Leiter des AK ist Rolf Blunk, Otaris. Die Mitwirkenden beschlossen die Erarbeitung einer "Handreichung 'Security by Design' für Unternehmer, Entscheider und Fach-Verantwortliche" mit Empfehlungs- und Definitionscharakter.

► TeleTrusT-Innovationspreis 2018 an MB connect line/Sonderpreis der Jury für DRACOON

Der 2018 zum 20. Mal verliehene TeleTrusT-Innovationspreis wurde an die MB connect line GmbH für die IT-Sicherheitslösung "mbNETFIX - Firewall für Automatisierer" vergeben. Den Sonderpreis der Jury erhielt die DRACOON GmbH für die Anwendung "DRACOON Enterprise Filesharing". Die Preisübergaben erfolgten am 06.11.2018 im Rahmen des T.I.S.P. Community Meetings (https://www.teletrust.de/tisp/tisp-community-meeting/) in Berlin.

Nominiert für den TeleTrusT-Innovationspreis 2018 waren aus insgesamt 20 Einreichungen u.a. auch Lösungen von Rohde & Schwarz, sayTEC, Genua, Delphix, DriveLock, FORTINET, Accellence und ITSG.

Der jährlich vergebene TeleTrusT-Innovationspreis wird Unternehmen oder Institutionen zugesprochen, die eine innovative, vertrauenswürdige und praxistaugliche IT-Sicherheitslösung entwickelt haben. Eine Jury wählt den Preisträger anhand folgender Kriterien aus:

- Ist das Sicherheitsniveau dem Schutzbedarf der Anwendung angemessen?
- Sind die Sicherheitsfunktionen integrierter Bestandteil des angebotenen oder genutzten Produktes?
- Sind die integrierten Sicherheitsfunktionen für den Anwender transparent und bedienerfreundlich?
- Ist die Anwendung interoperabel, idealerweise mit europäischer Reichweite?
- Trägt die Anwendung zur wirtschaftlichen Stabilität des Unternehmens bei?

www.teletrust.de/innovationspreis/teletrust-innovationspreis

► Neuer TeleTrusT-Vorstand

Auf der TeleTrusT-Jahresmitgliederversammlung 2018 - mit einer Rekordzahl an Teilnehmern - zog TeleTrusT positive Bilanz und stellte die Weichen für Aktivitäten im Jahr 2019. Mit kontinuierlichem Zuwachs an Neumitgliedern verzeichnet der Verband einen neuen Höchststand der Mitgliederzahl.

Die Mitgliederversammlung wählte turnusgemäß einen neuen Vorstand. Alter und neuer TeleTrusT-Vorsitzender ist Prof. Dr. Norbert Pohlmann (Institut für Internet-Sicherheit an der Westfälischen Hochschule). Wiedergewählt und zum stellvertretenden Vorsitzenden bestimmt wurde RA Karsten U. Bartels LL.M., HK2

Rechtsanwälte. Als neue TeleTrusT-Vorstände wurden Axel Deininger, Vorstand der secunet Security Networks AG und Dr. Kim Nguyen, Bundesdruckerei GmbH, gewählt.

Die scheidenden TeleTrusT-Vorstände Dr. Rainer Baumgart (Vorstandsvorsitzender secunet) und Ammar Alkassar (ehem. Rohde & Schwarz Cybersecurity, jetzt Bevollmächtigter für Innovation und Strategie in der Staatskanzlei des Saarlands) wurden mit herzlichem Dank für ihr langjähriges Engagement verabschiedet und bleiben TeleTrusT eng verbunden.

3 Veranstaltungen

► TeleTrusT mit Gemeinschaftsstand auf Intersec Dubai 2018

TeleTrusT und die Messe Frankfurt mit der Landesgesellschaft Middle East kooperierten im Dritten Jahr in Folge bei der Präsentation von "IT Security made in Germany" auf der Intersec 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 20. Intersec fand vom 21. - 23.01.2018 in Dubai (VAE) statt und führte als Messe mit begleitenden Veranstaltungen Entscheider und Verantwortungsträger aus Wirtschaft und Behörden zusammen.

► TeleTrusT als Partner der OMNISECURE 2018

TeleTrusT war erneut Partner der OMNISECURE vom 22. - 24.01.2018 in Berlin. Die OMNISECURE führt jährlich die wesentlichen Akteure aus Industrie und Politik zu den Themen Payment, Blockchain, elektronische Identitäten, Cyber Security, Smart Cities, eIDAS, eGovernment zusammen und verzeichnete in diesem Jahr 100 Referenten, 22 Foren, 12 Tutorials und Workshops sowie insgesamt 380 Teilnehmer.

► TeleTrusT auf dem Mobile World Congress Barcelona 2018

TeleTrusT war mit seiner Dachmarke "IT Security made in Germany" erneut Partner des NRW-Standes auf dem Mobile World Congress vom 26.02. bis 01.03.2018 in Barcelona, ES. Das Land Nordrhein-Westfalen ist dort wiederum mit einem Gemeinschaftsstand vertreten (Durchführungsgesellschaft Messe Düsseldorf). Die Partnerschaft mit Beteiligungsmöglichkeit insbesondere für KMU wird auch im kommenden Jahr fortgesetzt und erfasst von Seiten TeleTrusT Mitglieder mit Sitz in NRW, die die ITSMIG-Zeichenberechtigung haben.

► TeleTrusT unterstützte ECSO-"Investing Day for European Cybersecurity Companies" 2018

Im Rahmen der Mitträgerschaft und Mitwirkung bei der European Cybersecurity Organisation (ECSO) unterstützte TeleTrusT den "Investing Day for European Cybersecurity Companies".

► "Heise secIT" 2018 in Hannover in Partnerschaft mit TeleTrusT

TeleTrusT war Partner der neuen Veranstaltung "secIT", die von Heise Medien/Heise Events erstmalig am 06. - 07.03.2018 in Hannover ausgerichtet wurde. Diese IT-Sicherheitsveranstaltung will den Informationsaustausch von IT-Sicherheitsexperten und Entscheidern fördern und dabei mit Workshops und einer Ausstellung IT-Sicherheitsunternehmen bzw. Unternehmensvertretern eine Kommunikationsplattform bieten. Technische und wirtschaftliche Aspekte sollen gleichermaßen im Vordergrund stehen. Schwerpunktthemen sind u.a. Unternehmenssicherheit, Digitalisierung, IoT, Industrie 4.0, DSGVO und Endpoint Security.

► Infoabend im Kitzbühel Country Club zur EU-Datenschutzgrundverordnung

Gemeinsam mit der WTH Kitzbüheler Wirtschaftstreuhand veranstaltete TeleTrusT am 08.03.2018 einen Informationsabend zur EU-Datenschutzgrundverordnung:

https://www.teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dsgvo/kitzbuehel-country-club/

► TeleTrusT als Partner des "Landing Festival" 2018 in Berlin

TeleTrusT unterstützte als Teil der Nachwuchsförderung das "Landing Festival" in Berlin. Unter dem Slogan "Future. Tech. Careers - Tech Hiring" organisierte das "Landing Festival" am 14. und 15.03.2018 in Berlin die Begegnung von rd. 1.000 internationalen IT- bzw. IT-Sicherheitsexperten mit ausstellenden Unternehmen, die sich mit Job- und Karriereangeboten präsentieren. Das Event wurde von Vorträgen, Workshops, Expert Sessions und Panel-Diskussionen umrahmt.

► TeleTrusT-Regionaltreffen Stuttgart: "Stand der Technik gemäß DSGVO"

TeleTrusT und die Detack GmbH (TeleTrusT-Regionalstelle Stuttgart) luden zu einer Informations- und Diskussionsveranstaltung am 21.03.2018 zum Thema "Stand der Technik im Sinne der EU-Datenschutzgrundverordnung" in das Residenzschloss Ludwigsburg ein. Den Hauptvortrag hielt Tomasz Lawicki, (Schwerhoff Consultants), Leiter des TeleTrusT-AK "Stand der Technik" zum Thema "Stand der Technik gemäß DSGVO - Gesetzlich geforderter Technologiestand".

https://www.teletrust.de/ueber-teletrust/regionalstelle-stuttgart/

► TeleTrusT als Partner der Konferenz "IT-Sicherheit für KRITIS" 2018 in Berlin

TeleTrusT war Partner der Konferenz "IT-Sicherheit für KRITIS" am 10./11.04.2018 in Berlin. Als Referenten der Konferenz traten u.a. Vertreter von BMI, BKA, Verfassungsschutz, Bundeswehr, Telekom, Energieversorgern, Stadtwerken und Forschungseinrichtungen auf.

► Infoabend im Kitzbühel Country Club: Kryptogeld - Funktionsweise und steuerliche Behandlung

TeleTrusT in Kooperation mit der WTH Kitzbüheler Wirtschaftstreuhandgesellschaft informierten im Rahmen eines "Stubengespräches" im Kitzbühel Country Club über die technische Funktionsweise und die steuerliche Bewertung von Kryptogeld. Referenten des Abends waren Dr. André Kudra (esatus), Leiter der TeleTrusT-AG "Blockchain" und Dr. Hedwig Bendler (WTH Kitzbüheler Wirtschaftstreuhandgesellschaft).

https://www.teletrust.de/veranstaltungen/kryptogeld/

► TeleTrusT bei "Security Forum" 2018 in Hagenberg (AT)

TeleTrusT unterstützte über seine Regionalstelle FH Hagenberg (Oberösterreich) das "Security Forum 2018". Das Forum ist die jährliche IKT-Sicherheitskonferenz des "Hagenberger Kreises" und fand am 02./03.05.2018 in Hagenberg statt. An beiden Tagen wurden technische und managementorientierte Fachvorträge von Vertretern aus Wirtschaft, Forschung und öffentlicher Verwaltung gehalten. Am 03.05.2018 wurde zudem von der TeleTrusT-Regionalstelle Hagenberg zum zweiten Mal ein Treffen für die österreichischen TeleTrusT-Mitglieder veranstaltet.

► Netzwerktreffen "Start-ups"

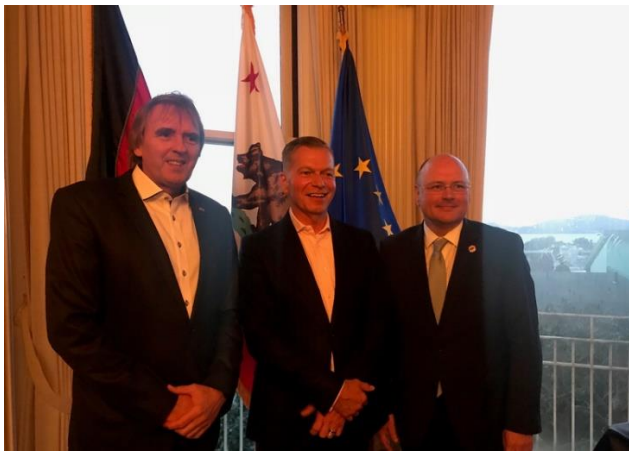
TeleTrusT, der Bundesverband Deutsche Start-ups und HK2 Rechtsanwälte Berlin richteten am 27.03.2018 in Berlin ein Netzwerk-Treffen für junge Unternehmen und Start-ups aus. Den Hauptvortrag hielt RA Karsten U. Bartels LL.M. (TeleTrusT-Vorstand und Leiter der TeleTrusT-AG "Recht" zum Thema "EU-Datenschutzgrundverordnung".

https://www.teletrust.de/veranstaltungen/netzwerktreffen-start-ups/

► RSA Conference 2018 in San Francisco: TeleTrusT präsentierte "IT Security made in Germany"

Vom 16.04. bis 20.04.2018 wurde in San Francisco/USA die 27. "RSA Conference" ausgerichtet. Die RSA ist nach wie vor die weltweit führende Messe bzw. Konferenz für IT-Sicherheit. Im "German Pavilion" präsentierte TeleTrusT mit 24 Verbandsmitgliedern "IT Security made in Germany". Es handelte sich um einen der größten und erfolgreichsten Gemeinschaftsauftritte der letzten Jahre. TeleTrusT organisierte ein umfangreiches Begleitprogramm.

https://www.teletrust.de/veranstaltungen/rsa/rsa-2018/



► TeleTrusT-Informationstag "IT-Sicherheit in der Landwirtschaft" 2018

So wie andere Wirtschaftsbereiche verändert die Digitalisierung auch die Landwirtschaft grundlegend. Informationstechnik ist inzwischen Teil des Alltags landwirtschaftlicher Betriebe. Hightech-Landmaschinen, automatisierte Arbeitsprozesse, Übermittlung sensibler Betriebsdaten: Damit einher gehen höhere Anforderungen an die IT-Sicherheit. TeleTrusT veranstaltete am 03.05.2018 in Berlin in Kooperation mit dem Verband der IT- und Internetwirtschaft in Berlin und Brandenburg e.V. (SIBB) und dem Deutschen Bauernverband e.V. (DBV) als ideellem Partner einen Informationstag zu aktuellen Herausforderungen der IT-Sicherheit für Landwirte und Landwirtschaftsbetriebe.

https://www.teletrust.de/veranstaltungen/landwirtschaft/

► TeleTrusT + Deutsch-Indische Handelskammer: Informationsveranstaltung zu Marktchancen in Indien

In Kooperation mit SBS systems for business solutions, der Deutsch-Indischen Handelskammer und weiteren Organisationen führte TeleTrusT am 08.05.2018 in Berlin eine Informationsveranstaltung zu "Geschäftschancen in Indien für zivile Sicherheitstechnologien und -dienstleistungen mit Fokus auf IT-Sicherheitstechnologien" durch. Berichtet wurde über das indische Marktpotential für einschlägige deutsche Unternehmen. Die 1-tägige Informationsveranstaltung fand im Rahmen des BMWi-Markterschließungsprogramms für KMU statt. Deutsche Mittelständler aus der zivilen Sicherheitstechnologiebranche wurden über Absatzchancen in Indien informiert. Fach- und Länderexperten aus Indien und Deutschland vermittelten Details über Zielmarkt und Branche, über rechtliche und steuerliche Besonderheiten, zur interkulturellen Kompetenz sowie konkrete Erfahrungen mit dem Indien-Geschäft. Das Angebot richtete sich vorwiegend an kleine und mittlere deutsche Unternehmen, Selbständige der gewerblichen Wirtschaft sowie fachbezogene Freie Berufe und wirtschaftsnahe Dienstleister.

► it-sa India 2018 in Mumbai mit Unterstützung von TeleTrusT

Analog zu der bereits etablierten it-sa Brasil in Sao Paulo fand am 24. und 25.05.2018 erstmalig eine it-sa India in Mumbai statt. Damit erweiterte die NürnbergMesse ihr Portfolio um eine weitere Fachmesse zum Thema IT-Sicherheit im Ausland. Das Projekt wird von TeleTrusT unterstützt.

https://www.teletrust.de/veranstaltungen/it-sa-india/it-sa-india-2018/

► Informationsveranstaltung: "IT Security made in Germany" - Opportunities for Cyber Security Companies within the U.S. Market

TeleTrusT organisierte in Kooperation mit der US-Botschaft in Deutschland, Fairfax County Development Authority und Select USA eine Informationsveranstaltung zu Marktchancen für deutsche IT-Sicherheitsunternehmen im US-Markt. Die Veranstaltung fand am 30.05.2018 in der US-Botschaft in Berlin statt.

https://www.teletrust.de/veranstaltungen/us-markt/

► "Cyber Security Challenge Germany 2018" mit Recruiting-Messe (Nachwuchsförderung)

Am 04.07.2018 fand die von TeleTrusT mitgetragene "Recruiting-Messe" der "Cyber Security Challenge Germany 2018" in Düsseldorf statt. Potentielle Arbeitgeber konnten sich dem interessierten IT-Sicherheitsnachwuchs präsentieren.

In der Cyber Security Challenge Germany werden Schüler und Studenten mit realistischen Cyber-Angriffen konfrontiert und vor Herausforderungen gestellt. Der Wettbewerb richtet sich an Teilnehmer zwischen 14 und 25 Jahren. Schüler und Studenten können jederzeit einsteigen, um die Aufgaben ("Challenges") bis zum Stichtag zu lösen. Mit der "Cyber Security Challenge Germany" soll das inländische Qualifikationspotential in der IT-Sicherheit ermittelt und gefördert werden. 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.

► TeleTrusT als Partner der Infosecurity Europe 2018

TeleTrusT war als Partner der Infosecurity Europe 2018 in London vom 05. - 07.06.2018 mit einem Gemeinschaftsstand vertreten. Die "Infosecurity Europe" (Infosec) ist europaweit eine der größten Messen im Bereich der Informationssicherheit. Mit einem begleitenden Konferenzprogramm und über 400 Ausstellern sowie einer beachtlichen Besucherzahl wurden informationssicherheitsrelevante Produkte und Lösungen auf der Infosec präsentiert. TeleTrusT koordinierte auf der Infosecurity den Gemeinschaftsstand "IT Security made in Germany".

https://www.teletrust.de/veranstaltungen/infosecurity/infosecurity-2018/

► FIDO Alliance + TeleTrusT: "Strong Authentication Workshop" 2018

Die FIDO Alliance und TeleTrusT veranstalten am 02.07.2018 in Berlin einen Gemeinschaftsworkshop zu "Future of strong authentication":

- FIDO 101: A primer on FIDO Authentication
- Specification Overview: An in-depth look at FIDO specifications
- Deployment case studies: Hands-on insights from organizations that have deployed FIDO
- The European Market Perspective: A look at how FIDO Authentication provides solutions to the regulatory challenges posed by PSD2 and GDPR

https://www.teletrust.de/veranstaltungen/tutorials-workshops/teletrust-fido/teletrust-fido-workshop/

► TeleTrusT-EBCA/PKI-Workshop

Der diesjährige TeleTrusT-EBCA "PKI-Workshop" widmete sich Aspekten, die rund um das Thema PKI angesiedelt sind und beleuchtete den Stand der Technik sowie neueste Entwicklungen. 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 (Berlin, 26.06.2018).

https://www.teletrust.de/veranstaltungen/tutorials-workshops/ebca-pki-2018/

► TeleTrusT als Partner der "ditact women's IT summer studies" 2018 in Salzburg

TeleTrusT war erneut Partner der "ditact women's IT summer studies" 2018 vom 20.08. - 01.09.2018 an der Universität Salzburg. Interessierten Frauen wurden Kurse geboten, die einen Einblick in die Welt der IT geben und die aktuellen Trends berücksichtigten. Das Programm der ditact war in sechs große Themengebiete aufgeteilt: IT-Grundlagen, IT-Spezialisierung, IT-Anwendungen, IT-Management, IT & Didaktik, IT & Karriereplanung.

► TeleTrusT als Partner des "German-Japanese Defense and Technology Forum" 2018 in Tokio

TeleTrusT war Partner des "German-Japanese Defense and Technology Forum" am 25./26.09.2018 in Tokio, JP. Organisator war die Deutsche Außenhandelskammer in Japan mit Unterstützung der Deutschen Botschaft in Tokio.

► TeleTrusT-Informationstag "Blockchain" 2018

Mit dem fortschreitenden Diskurs und neuen Entwicklungen auf dem Gebiet "Blockchain" rücken vielfältige Anwendungsmöglichkeiten in den Fokus. TeleTrusT veranstaltete am 27.06.2018 in Berlin den diesjährigen TeleTrusT-Informationstag "Blockchain", um das Thema mit Blick auf mögliche Anwendungsfälle - auch jenseits der bereits etablierten kryptografischen Währung Bitcoin - fachlich vertieft zu behandeln.

https://www.teletrust.de/veranstaltungen/blockchain/blockchain-2018/

► TeleTrusT-interner Workshop 2018

Der diesjährige TeleTrusT-interne Workshop (IWS) fand am 05./06.07.2018 in Berlin statt. Gastgeber war Siemens. Im Rahmen des Workshops wurden Impulsvorträge gehalten, gefolgt durch Fachdiskussionen. Der IWS bot Gelegenheit, gemeinsam die fachliche Fortentwicklung des Verbandes zu erörtern.

https://www.teletrust.de/veranstaltungen/tutorials-workshops/teletrust-iws-2018/

► TeleTrusT und Cluster Mechatronik + Automation: Kooperationsworkshop "Industrial Security in der Automatisierungspraxis"

Wie bereits in den Vorjahren luden TeleTrusT und das Bayerische Cluster Mechatronik + Automation zum Kooperationsworkshop "Industrial Security in der Automatisierungspraxis" ein (04.10.2018, Hosokawa Alpine AG, Augsburg)

Die von den Referenten freigegebenen Präsentationen sind hier abrufbar: https://www.teletrust.de/veranstaltungen/tutorials-workshops/industrial-security-2018/

► TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste" 2018

TeleTrusT und der TeleTrusT-Partnerverband Organisations- und Informationssysteme e.V. (VOI) organisierten auf dem traditionellen gemeinsamen Informationstag "Elektronische Signatur und Vertrauensdienste" (Signaturtag) am 18.09.2018 in Berlin Vorträge, Gruppendiskussionen und moderierte Streitgespräche zu Trendthemen rund um die E-Signatur. Experten aus Wirtschaft, Verwaltung und Forschung erörterten in Impulsvorträgen die aktuelle Situation der elektronischen Signatur und der elektronischen Vertrauensdienste.

Mit der Veranstaltungsreihe wird eine Plattform geboten, auf der neben neuesten Informationen rund um die elektronische Signatur und Vertrauensdienste vor allem der Austausch mit den Teilnehmern im Vordergrund steht. Dies findet wie im vergangenen Jahr in Form einer "eSig-Kontaktanbahnung" statt. Die Gestaltung des Programms ermöglicht, Herausforderungen und Fragen aus dem eigenen Arbeitsumfeld zu diskutieren. Der Teilnehmerkreis der Veranstaltung besteht regelmäßig aus Unternehmens-, Behörden- und Forschungsvertretern bzw. Informatikern, Juristen und Betriebswirtschaftern, was zu interdisziplinärem Meinungsaustausch beiträgt.

Kernthemen 2018 waren aktuelle Entwicklungen im Bereich Innovation Banking sowie Signaturanwendungen in Zusammenhang mit Blockchain. Der Themenbereich Recht mit einem aktuellen Statusbericht zur Ausarbeitung der Vertrauensdienste-Verordnung sowie Praxisvorträgen zu eIDAS und Datenschutzgrundverordnung rundete das Programm ab.

www.teletrust.de/veranstaltungen/signaturtag/infotag-elektronische-signatur-und-vertrauensdienste-2018/

► TeleTrusT: IT-Sicherheitsrechtstag 2018 / "Umsetzung von DSGVO und ITSiG in der Praxis"

Die Umsetzung gesetzeskonformer IT-Sicherheit in Unternehmen, öffentlichen Stellen und Behörden erfordert zahlreiche technische, organisatorische und rechtliche Maßnahmen. So stellt die Datenschutz-Grundverordnung (DSGVO) seit dem 25.05.2018 deutlich erhöhte Anforderungen an den technischen Datenschutz. Das IT-Sicherheitsgesetz gilt bereits seit 2015.

TeleTrusT präsentierte im Rahmen einer interdisziplinären Informationsveranstaltung am 25.10.2018 in Berlin Erfahrungen, Lösungsansätze und Praxistipps. Im Fokus standen die Möglichkeiten der erfolgreichen Umsetzung gesetzlicher IT-Sicherheits- und Datenschutzanforderungen in der Unternehmens- und Behördenpraxis. Unter anderem mit dem IT-Sicherheitsgesetz und der DSGVO haben die Gesetz- und Verordnungsgeber auf nationaler und europäischer Ebene wichtige regulatorische Vorgaben gesetzt. Unternehmen und Behörden sind aufgefordert, ihre Strukturen sowie die technischen, organisatorischen und rechtlichen Maßnahmen zu überprüfen und unter Berücksichtigung des Standes der Technik anzupassen. Insbesondere sind die Maßnahmen und Verfahren umfänglich zu dokumentieren.

Referenten aus der technischen, juristischen, betrieblichen, aufsichtsbehördlichen und gutachterlichen Praxis, einschließlich der Landesdatenschutzbeauftragten Niedersachsen, erörterten die praxisrelevanten Herausforderungen der datenschutzrechtlichen und IT-sicherheitsgesetzlichen Obliegenheiten.

https://www.teletrust.de/veranstaltungen/it-sicherheitsgesetz-und-dsgvo/it-sicherheitsrechtstag-2018

► TeleTrusT-Mitgliederkonferenz 2018

Im Vorfeld der TeleTrusT-Mitgliederversammlung 2018 wurde am 29.11.2018 eine TeleTrusT-Mitgliederkonferenz zu aktuellen Perspektiven der IT-Sicherheit ausgerichtet.

https://www.teletrust.de/veranstaltungen/mitgliederkonferenz/

► TeleTrusT-Gremiensitzungen 2018

■ 30.01.2018, Düsseldorf: TeleTrusT-EBCA-Board-Sitzung (bei Uniper/E-On)
■ 26.02.2018, Berlin: TeleTrusT-Vorstandssitzung
■ 21.03.2018, Darmstadt: TeleTrusT-AG "Biometrie"
■ 26.03.2018, Berlin: TeleTrusT-AG "Smart Grids/Industrial Security"
■ 17.04.2018, Berlin: TeleTrusT-EBCA-AG-"Technik"
■ 24.04.2018, Berlin: TeleTrusT/T.P.S.S.E.-Lenkungsgremium
■ 16.05.2018, Berlin: TeleTrusT-EBCA-Board + EBCA-AG "Technik"
■ 07.06.2018, Berlin: TeleTrusT-AG "Smart Grids/Industrial Security"
■ 04.07.2018, Berlin: TeleTrusT-AG "RSA 2019"
■ 23.08.2018 (Telko): T.I.S.P.-Lenkungsgremium
■ 20.09.2018, Berlin: EBCA-AG "Technik"
■ 26.09.2018, Darmstadt: TeleTrusT-AG "Biometrie"
■ 17.10.2018, Essen: EBCA-Lenkungsgremium
■ 26.10.2018, Berlin: TeleTrusT-AG "RSA 2019"
■ 05.11.2018, Hannover: TeleTrusT-AK "Mail Security"
■ 12.11.2018, Berlin: TeleTrusT-AK "Stand der Technik"
■ 21.11.2018, Berlin: TeleTrusT-Vorstandssitzung (Telko)
■ 30.11.2018, Berlin: TeleTrusT-Mitgliederversammlung (am Vortag Mitgliederkonferenz)
■ 11.12.2018, Berlin: TeleTrusT-AG "Biometrie"

► TeleTrusT-Eigen- und Kooperationsveranstaltungen 2018

■ 26.02.2018, Berlin: TeleTrusT-Neujahrsempfang
■ 21.03.2018, Stuttgart: TeleTrusT-Regionaltreffen Stuttgart (in Kooperation mit Detack, TeleTrusT-Regionalstelle Stuttgart)
■ 27.03.2018, Berlin: Offenes Netzwerktreffen für Start-ups, in Kooperation mit dem Bundesverband Deutsche Start-ups und HK2 RAe
■ 27.04.2018, Kitzbühel: Informationsabend im Kitzbühel Country Club: "Kryptogeld - Funktionsweise und steuerliche Behandlung"
■ 03.05.2018, Berlin: Informationstag "IT-Sicherheit in der Landwirtschaft", in Kooperation mit dem Verband der IT- und Internetwirtschaft in Berlin und Brandenburg e.V. und dem Deutschen Bauernverband e.V.)
■ 30.05.2018, Berlin: "IT Security made in Germany" - Opportunities for Cyber Security Companies within the U.S. Market (In Kooperation mit Fairfax County Economic Development Authority, Select USA und US-Botschaft Deutschland)
■ 26.06.2018, Berlin: TeleTrusT-EBCA-"PKI-Workshop"
■ 27.06.2018, Berlin: TeleTrusT-Informationstag "Blockchain"
■ 05./06.07.2018, Berlin: TeleTrusT-interner Workshop 2018
■ 26.06.2018, Berlin: TeleTrusT-EBCA-"PKI-Workshop"
■ 02.07.2018, Berlin: TeleTrusT/FIDO Alliance Workshop
■ 03.07.2018, Berlin: Beuth/DIN + TeleTrusT - "DachgartenTalk"
■ 04.07.2018, Düsseldorf: "Cyber Security Challenge Germany 2018" mit Recruiting-Messe
■ 18.09.2018, Berlin: TeleTrusT/VOI-Informationstag "Elektronische Signatur und Vertrauensdienste"
■ 03.10.2018, München/Hallbergmoos: "Industrial Security in der Automatisierungspraxis", in Kooperation mit dem Bayerischen Cluster Mechatronik & Automation
■ 04.10.2018: "Industrial Security in der Automatisierungspraxis", in Kooperation mit dem Cluster Mechatronik & Automation
■ 09.10. - 11.10.2018, Nürnberg: Begleitprogramm zur it-sa 2018
■ 25.10.2018, Berlin: TeleTrusT-"IT-Sicherheitsrechtstag"
■ 06./07.11.2018, Berlin: TeleTrusT/T.I.S.P. Community Meeting 2018
■ 29.11.2018, Berlin: TeleTrusT-Mitgliederkonferenz
■ 30.11.2018, Berlin: TeleTrusT-Mitgliederversammlung

4 Neue Kooperationen

► TeleTrusT Premium Partner der it-sa Nürnberg

TeleTrusT ist jetzt Premium Partner der IT-Sicherheitsfachmesse it-sa und bekennt sich damit in Kontinuität zum schon bisherigen Engagement zur it-sa als nationaler Leitmesse für IT-Sicherheit. Eine entsprechende Vereinbarung wurde mit der NürnbergMesse geschlossen. TeleTrusT wird weiterhin und nunmehr verstärkt die inhaltliche Gestaltung der it-sa und des begleitenden Rahmenprogramms prägen. Dazu zählen auch der Gemeinschaftsstand für Verbandsmitglieder und die Mitwirkung im Messebeirat.

► TeleTrusT jetzt Mitglied im North European Cybersecurity Cluster (NECC)

Als Erweiterung der Netzwerk-Aktivitäten auf europäischer Ebene ist TeleTrusT dem neu etablierten North European Cybersecurity Cluster (NECC) beigetreten, in dem sich IT-Sicherheitsverbände Nordeuropas zu einem "Nordic Cluster" zusammengeschlossen haben. Organisatorisch federführend ist der finnische TeleTrusT-Partnerverband FISC. TeleTrusT war von dort um Mitwirkungsinteresse angefragt worden. Das Cluster kann u.a. gemeinsam auf EU-Ausschreibungen reagieren.

Ähnlich wie das Engagement bei der European Cybersecurity Organisation (ECSO) wird sich TeleTrusT einbringen und den gezogenen Nutzen in absehbarer Zeit evaluieren.

► TeleTrusT als Partner des Information Security Network im IT-Cluster Oberösterreich

TeleTrusT und das Information Security Network des IT-Clusters der Business Upper Austria (IT-Cluster OÖ) haben die Partnerschaft vereinbart. Das IT-Cluster ist das größte österreichische Kooperationsnetzwerk der IT-Branche und Teil der Business Upper Austria, der oberösterreichischen Standortagentur. Kontakte des IT-Clusters zu mehr als 170 Partnerunternehmen schaffen Raum für Erfahrungsaustausch, Kooperation und Innovation. Ein Themenschwerpunkt ist Informationssicherheit und Datenschutz.


TeleTrusT
Pioneers in IT security.