ZVEI: Die Elektroindustrie

Notwendige Weiterentwicklung der Cybersicherheit in Europa

Impulse für die Bundestagswahl 2017

Januar 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Inhalt

Grundsätze der Elektroindustrie

Die Elektroindustrie ist eine exporttreibende Branche, die auf offene Märkte, internationale Vernetzung und weltweit kompatible Richtlinien angewiesen ist. Zudem ist sie durch die Bereitstellung von Intelligenz in Sensoren, Steuerungen und Systemen eine ungemein wissensintensive B2B orientierte Branche. Viele ZVEI-Mitglieder sind Weltmarktführer in ihrem Segment. Der Schutz der Unternehmen sichert bis zu 800.000 Arbeitsplätze und Spitzen-Know-how. Industrietaugliche Initiativen und Regulierungen in Berlin und Brüssel sind angesichts der spezifischen Rahmenbedingungen unerlässlich. Vor diesem Hintergrund spricht sich die Elektroindustrie für folgende grundsätzliche Anliegen aus:

- **Beteiligung der Hersteller am UP KRITIS**: Die Sicherheitsarchitektur Europas wird erst dann passen, wenn die Security-Anforderungen der (Infrastruktur-)Betreiber durch die Security-Fähigkeiten der Produkte und Systeme abgebildet werden können. Eine „top-down"-Definition der Anforderungen durch Behörden und Betreiber allein greift daher zu kurz. Hersteller sind insofern an Plattformen wie dem UP-KRITIS in geeigneter Weise zu beteiligen.
- **Industriekontext bedenken:** Die Vertragsmöglichkeiten, Haftungsregelungen, Produktzyklen, Kundenbeziehungen, Softwarerelevanz und Normenorientierung formen die Cybersicherheit in der Industrie anders als in der Office-IT. Dieses Anwendungsfeld muss die Politik bei ihrer Sicherheitsregulierung berücksichtigen.
- **Sektorspezifische Ansätze zulassen:** Durch die unterschiedlichen Rahmenbedingungen und Anforderungen sind die Produkte und Systeme der Elektroindustrie äußerst divers. Vorschriften und Standards lassen sich nur bedingt auf mehrere Sektoren übertragen. Konzepte für die Cybersicherheit müssen für den jeweiligen Sektor adaptierbar sein. Das IT-Sicherheitsgesetz gibt ein gutes Vorbild.
- **Exportfähigkeit gewährleisten:** Regelungen für Cybersicherheit sollten stets auf internationalen Standards aufbauen. Die Elektroindustrie produziert für den Weltmarkt. Unweigerlich schwächen nationale Vorschriften den Industriestandort.
- **Industrial Security etablieren:** Vernetzte Industrien müssen geschützt werden, um Wertschöpfung zu sichern. Dies erfordert „Industrial Security"-Knowhow speziell für den Industriekontext. Durch Forschungs- und Studienförderung sowie Investitionshilfen sollte die Politik Industrieanwender und Anbieter stärken und helfen, diesen integralen Sektor aufzubauen.

Europa ist der natürliche Bezugsrahmen der exportstarken deutschen Elektroindustrie. Für die EU fehlt jedoch bisher ein gemeinsames Bild für das Gesamtsystem. Die Zielvorstellung des ZVEI ist eindeutig.

Die **Europäische Union ist zu einem gemeinsamen Vertrauensraum** mit den Schwerpunkten Cybersicherheit und Datenschutz auszubauen. Ziel sollte der Aufbau einer Infrastruktur sein, die es erstmals erlaubt, Identitäten, Kommunikationsbeziehungen und Daten vertrauenswürdig zwischen Menschen, Maschinen und Komponenten zu verifizieren und auszutauschen.

Cybersicherheit wird zum integralen Bestandteil der Digitalisierung. Denn rückwirkend lässt sich Sicherheit nur sehr schwer und teuer implementieren. In der Konsequenz bedeutet dies, dass jeder Grün- und Weißbuchprozess der Ministerien sowie deren Plattformen Cybersicherheit von Beginn an selbstverständlich aufgreifen sollten. Aktuell ist das noch nicht ausreichend der Fall.

Staatliche Handlungsfelder

In der staatlichen Verantwortung liegt der Schutz der Öffentlichkeit und der kritischen Infrastrukturen. Zusätzlich geht es um die Förderung des Industriestandortes Deutschland. Die Cybersicherheit übernimmt hierfür eine Doppelrolle. Einerseits sichert sie Industrie-Know-how, Wertschöpfung und damit Arbeitsplätze für alle Wirtschaftsteilnehmer. Andererseits fördern Sicherheitsanbieter die Innovationskraft, Unabhängigkeit und Wahlfreiheit der europäischen Wirtschaft. Die Stärkung des europäischen Cybersicherheitsmarktes ist daher Sicherheits-, Standort- und Innovationspolitik zugleich.

Zulassungs- und Zertifizierungsverfahren beschleunigen

Zur Stärkung des Cybersicherheitsmarktes in Deutschland und Europa sind marktgerechte Zyklen maßgeblich. Die Prüf- und Zulassungsverfahren von Sicherheitsprodukten müssen marktgerecht sein. Zum Beispiel wirkt sich die durchschnittliche Dauer einer gemäß *Common Criteria* (CC) Standard durchgeführten Zertifizierung im Halbleiterbereich von ca. sechs Monaten hinderlich für deutsche Anbieter aus. Hinzu kommt der Zeitaufwand für die Systemimplementierung. Ein europäischer Markt gelingt nur, wenn die Mitgliedstaaten sich an vergleichbaren – bestenfalls international kompatiblen Standards – orientieren. Generell ist eine gestufte Zertifizierungsmöglichkeit unterhalb der CC-Anforderung, zum Beispiel nach dem französischen Vorbild (siehe ANSSI Lightweight Zertifizierung), erstrebenswert.

- *Das Bundesamt für Sicherheit in der Informationstechnik (BSI) sollte durch das Bundeskabinett ein klares Mandat erhalten,*
  - den Prozess für die Lightweight-Zertifizierung eng zu begleiten,

- *eine Übertragung auf Deutschland zu ermöglichen und*
- *das Vorhaben über Partner wie z.B. ENISA einheitlich auf die EU zu übertragen.*

- *Dem BSI sind mehr Personen und Mittel für die Zertifizierungsverfahren zur Verfügung zu stellen. Ziel sollte sein, die durchschnittliche Bearbeitungszeit auf drei Monate zu senken.*
- *Bei der Akkreditierung privater Zertifizierungsstellen durch das BSI ist verstärkt auf eine ausreichende Prüfkompetenz, Effizienz und Ausstattung der Anbieter zu achten. Gleichfalls ist stets auf eine Balance zwischen Geschäftsmodellen, Aussagekraft der Zertifikate und Nachweispflichten für Sicherheitsprodukte zu achten.*

Export-Genehmigungsverfahren neu strukturieren

Deutschlands Stärke bleibt bis auf weiteres der Export - auch von zivilen Sicherheitsgütern. Er sichert Arbeitsplätze und fördert die Innovationskraft hierzulande. Entsprechend nehmen Genehmigungsverfahren Einfluss die Wettbewerbsfähigkeit des Standorts. Zu Recht bestehen umsichtige Regelungen für den Export von Sicherheitsgütern. Die größten Mühen erzeugen nicht die Regeln selbst, sondern die Intransparenz der Bearbeitungsverfahren. Hersteller können die Dauer und Verlässlichkeit des Prozesses kaum einschätzen. Es fehlen „Regelbearbeitungszeiten“ an denen sich Unternehmen und Kunden orientieren können. Auch eine Statusabfrage für den Exportantrag ist im Regelfall über einen zentralen Prozess nicht möglich. Wenn Hersteller ihren Kunden keinerlei Informationen zu der erwarteten Bearbeitungsdauer und damit zum Erhalt des Produkts geben können, schädigt dies die Wettbewerbsfähigkeit unmittelbar.

- *Das Bundesamt für Wirtschaft und Ausfuhrkontrolle möge als zentrale Anlaufstelle der Unternehmen eine Regelbearbeitungszeit einführen und Statusabfragen ermöglichen. Angesichts internationaler Vergleichswerte sollte das Ziel eine Dauer von unter drei Monaten sein.*
- *Zusätzlich sind kurzfristig personelle Engpässe auf Seiten der Genehmigungsbehörden zu schließen, um nachteilige Zeitverzögerung bei der Antragsbearbeitung zu vermeiden.*
- *Die Bundesregierung möge Sorge tragen, dass der Dual-Use-Anwendungsbereich stets verhältnismäßig bleibt. Eine zu große Ausweitung auf zivile IT-Sicherheitsprodukte schwächt die Anbieter- und Anwenderseite gleichermaßen.*
- *Nachsendungen von Sicherheitsgütern (z.B. im Kontext von Reparaturen und Wartungen von Maschinen) sollten deutlich aufwandsärmer möglich sein, als die Erstausfuhr eigenständiger Sicherheitsgüter.*

Finanzielle Anreize für Security-Innovationen schaffen

Für die Industrie sind angesichts beschränkter Ressourcen Hilfestellungen wichtig, um Investitionen in Sicherungsmaßnahmen voranzutreiben. Derzeit werden immaterielle Investitionen, wie zum Beispiel Awareness- und Ausbildungsprogramme, nicht ausreichend von Finanz- und Versicherungsinstitutionen berücksichtigt.

- *Die steuerliche Forschungsförderung ist ergänzend zur Projektförderung von der Bundesregierung einzuführen.*
- *Die Bundesregierung wird zusammen mit den Banken- und Versicherungsverbänden aufgefordert, Bewertungsstandards für immaterielle Investitionen in ihre Richtlinien zu integrieren, um die Kreditvergabe für Industrieunternehmen zu erleichtern. Derartige Maßnahmen sollten sich positiv auf die Kreditwürdigkeit auswirken, da sie die jeweiligen Investitionen insgesamt besser schützen.*

Interdependenz zwischen Cybersicherheit und Funktionaler Sicherheit bedenken

In Europa besteht ein tiefgreifendes Regelwerk für die funktionale Sicherheit (engl. Safety). Funktionale Sicherheit beinhaltet Maßnahmen zur Vermeidung von Gefährdungen von Leben, Gesundheit und Umwelt durch Maschinen und Systeme. Zur Gewährleistung der funktionalen Sicherheit ist es unter anderem untersagt, Softwarestände oder Konfigurationen in Maschinen zu ändern. Ein notwendiger Security-Patch ist daher zuweilen untersagt. Auch kann z.B. ein Maschinenbetreiber in die Verlegenheit kommen, nach dem Patchen eine neue Zertifizierung der Anlage durchführen zu müssen. Folglich können Soft- und Hardwarehersteller auch nicht vorbehaltlos in jedem Fall Security-Patches bereitstellen bzw. durchführen.

- *Die Ausgestaltung der im IT-Sicherheitsgesetz formulierten Herstellerverantwortung „Pflicht zur unverzüglichen Vorfallbehebung und Hilfestellung“ (§ 8b 6) ist vor dem Hintergrund der geschilderten Rahmenbedingungen in enger Kooperation mit den Herstellern vorzunehmen.*
- *Politik und Industrie können gemeinsam Wege zur Gewährleistung der Rückwirkungsfreiheit von funktionaler Sicherheit und Cybersicherheit finden. Das „New Legislative Framework“ der EU, das die Normung zur Ausgestaltung regulativer Anforderungen vorsieht, sollte bei der Umsetzung primär Anwendung finden.*
- *Die Rolle des Inverkehrbringens eines Produktes werden sich unter den Geboten der Cybersicherheit in Europa anpassen müssen. Ein „Sell and forget“ wird sich im Sinne einer (bezahlten) Security-Gewährleistung fortentwickeln. Diesen Prozess umsichtig zu gestalten ist gemeinsame Aufgabe von Politik und Wirtschaft.*

Sichere Industriekommunikation ermöglichen

Kunden und Anbieter müssen ihren digitalen Ressourcen und Daten vertrauen können. Eine bewusste behördliche Schwächung von Sicherheitsstandards und Technologien lehnt der ZVEI entschieden ab. Eine Ende-zu-Ende-Sicherheit der Privat- und Industriekommunikation muss über verschiedene Infrastrukturen hinweg möglich sein.

- *Die Bundesregierung ist aufgefordert, für dieses Ziel bei anderen Partnerstaaten einzutreten und hierzulande defensive und offensive Cyberkompetenzen behördlich klar zu trennen.*

Keine Verengung der Sicherheitsmaßnahmen auf Verschlüsselung

Kryptologie-Technologie aus Deutschland findet international hohe Anerkennung. Die Politik fördert diesen Bereich durch Initiativen wie „Volksverschlüsselung“ oder mit der Fokusgruppe „Sichere und handhabbare Verschlüsselung für Jedermann“ im IT-Gipfel Prozess. Die Maßnahmen leisten einen Beitrag und werden seitens des ZVEI begrüßt. Eine reine Verschlüsselung des Kommunikationskanals sichert jedoch nicht die Inhalte, Metadaten oder die Daten in den Endsystemen. Sind Daten und Kommunikationswege bereits korrumpiert, wenn sie den verschlüsselten Kanal betreten, werden sie ungehindert weitergeleitet und sind sogar schwerer zu detektieren. Sicherheit muss als Prozess und durchgängig von Datenerhebung, -bearbeitung, -speicherung, -transport und -visualisierung über Hard- und Softwareplattformen hinweg verstanden und gefördert werden.

- *Initiativen für sichere Identitäten, Authentifizierung, Detektions- und Bewertungskompetenz sollten im gleichen Maße angestoßen und gefördert werden wie Projekte für Verschlüsselung.*
- *Der zukünftige Digitalisierungs-Gipfel, die Forschungsförderung und staatliche Awareness-Plattformen sollten alle Facetten der Sicherheit abdecken und Maßnahmen für die Bevölkerung vorschlagen. Keine dieser Initiativen sollte einen Teilaspekt der Sicherheit gesondert fördern.*

Zusammenführung behördlicher Awareness-Plattformen

Die Cybersicherheit darf nicht durch ein verwirrendes Tätigkeitsprofil der Ministerien geschwächt werden. Die durch einzelne Bundesministerien geförderten Initiativen „IT-Sicherheit in der Wirtschaft“, „Initiative Wirtschaftsschutz“ und die „Allianz für Cybersicherheit“ verfolgen vergleichbare und sich zum Teil überlappende Ziele. Ergänzt man die Plattformen der Bundesländer, entsteht für Unternehmen ein verwirrendes Bild. Auf diese Weise wird die Aufmerksamkeit der Unternehmen gemindert und es gehen klare Ansprechpartnerstrukturen verloren.

- *Die Bundesregierung möge die genannten Initiativen zusammenführen oder zumindest für eine klare Aufgaben- und Zielgruppenteilung sorgen.*
- *Ein gebündeltes, konzentriertes Auftreten, zum Beispiel mit übergreifenden Maßnahmen im Rahmen des Monats der Cybersicherheit (EU-Initiative jeweils im Oktober des Jahres), sollte ausgebaut werden.*

Gemeinsame Handlungsfelder von Staat und Unternehmen

Eine Stärkung der Cybersicherheit können Politik und Industrie nur gemeinsam erreichen. Ein Pooling an Ressourcen, Know-how, Monitoring und Investitionen ist ebenso erforderlich, wie die gemeinsame Festlegung von strategischen Ansatzpunkten für Forschung und Technologieentwicklung. Internationale Entwicklungen in der Normung, technische Entwicklungen und Marktverschiebungen prägen die Marktbedingungen von morgen. Gleichzeitig stellen sie die Weichen für die dominierenden Basistechnologien und IT-Infrastrukturen mit weitreichenden Auswirkungen auf die sicherheitsrelevante Selbstbestimmung von Bürgern, Unternehmen und Behörden. Es gilt, gemeinsam zielgerichtete Fördermaßnahmen zu definieren und durch einen starken Heimatmarkt Sicherheitstechnologien für Bürger und Industrie hierzulande konkurrenzfähig zu etablieren.

Strategisch bedarf es einer Normung, die Hardware und Software verbindet, Prozesse und Produktlebenszyklen einschließt und effektive Anwendung findet. Gleichzeitig müssen neue technische Entwicklungen Berücksichtigung finden und dies technologieneutral sowie innovationsoffen. In die Standardisierung sollte insbesondere „*Security-by-Design*“ (auch hinsichtlich der Unterstützerrolle für den Datenschutz) als wesentliches Grundprinzip von Beginn an in die technische Fortentwicklung mit einfließen. Wirtschaft und Politik können zusätzlich geeignete Wege definieren, Sicherheitseigenschaften und -niveaus von Produkten für den Endanwender kenntlich zu machen und auf diese Weise seine Handlungsfreiheit zu stärken. Die Elektroindustrie steht für den Austausch bereit.

Regionale Showrooms für „Stand der Technik Security“

Wenn KMUs beginnen, sich mit Security-Maßnahmen auseinanderzusetzen, fällt ihnen häufig die Übersicht schwer. Die Frage, was sinnvoll als Standardmaßnahmen einzusetzen ist, bleibt häufig offen. Virtuelle Showrooms (z.B. Website, online Plattform), über die sich Unternehmer anwenderorientiert über den „Stand der Technik“ informieren können, schaffen leicht zugängliche Abhilfe.

Zusätzlich können die sieben Mittelstand 4.0-Kompetenzzentren in Berlin, Chemnitz, Darmstadt, Dortmund, Hannover, Ilmenau und Kaiserslautern sowie das

Kompetenzzentrum Digitales Handwerk als Darstellungsplattformen und Vertiefung dienen. Sie adressieren Mittelständler und haben bewusst einen Industrie-schwerpunkt.

- *Die Bundesregierung möge ein Budget für die Sondierung, Prüfung und virtuelle-didaktische Aufbereitung des Stands der Technik für Cybersicherheit bereitstellen.*
- *Die Allianz für Cybersicherheit kann als kooperative Plattform von Politik, Anbietern und Anwendern in der Industrie die Umsetzung des Auswahlkonzeptes qualitativ und ausreichend unabhängig vornehmen.*

Initiative von Wirtschaft und Staat für eine neue Identitäten-Infrastruktur

Identitäten und Authentifizierung von Menschen, Maschinen und Komponenten werden im Zeitalter des Internets der Dinge und Dienste die Grundlage für jegliche Sicherheitsmaßnahmen legen (müssen). Aktuell können Unternehmen innerhalb ihres Verantwortungsbereichs Identitäten leicht vergeben und austauschen. Unternehmens- und vor allem sektorenübergreifend stellt dies jedoch eine enorme Herausforderung dar. Allein durch unterschiedliche Sicherheits-Policies müssen zwei in sich vertrauenswürdige Unternehmen einen ungemeinen Zeit- und Personalaufwand betreiben, um sich zu einem vertrauenswürdigen Netzwerk zusammenzuschließen. Das erzeugt Ineffizienzen, Aufwand und Wertschöpfungs-verluste. In national und international benötigen wir eine allgemeine vertrauens-würdige Basisinfrastruktur, die die Identität von Unternehmen glaubwürdig und sicher bestätigt, so dass die Unternehmen diese Originalbestätigung an ihre Mitarbeiter, Maschinen und ggf. Komponenten weitergeben können. Auf diese Weise würde eine Vertrauensgrundlage für alle künftigen Aktions-, Vertrags- und Wirtschaftsbeziehungen, insbesondere im Kontext von autonomen Systemen und Industrie 4.0, entstehen. Diese Funktion ist so grundlegend, dass sie jedem Wirtschaftsakteur anwenderfreundlich und effizient zur Verfügung gestellt werden muss. An dieser Stelle ergibt sich eine gemeinsame Handlungsbasis für Staat und Wirtschaft.

- *Die Arbeiten der Plattform Industrie 4.0 zum Thema sind zu unterstützen und im Anschluss politisch zu flankieren.*
- *In einem erweiterten Dialogformat sollten Ideen sowie ein gestuftes Migrations- und Umsetzungskonzepte zwischen Industrie- und Behörden-vertretern erarbeitet werden.*
- *Aufgrund des notwendigen grundlegenden und flächendeckenden Charakters der Infrastruktur sind Überlegungen einer Aufbaufinanzierung durch Steuermittel ergebnisoffen zu prüfen.*

Umsichtiger Einsatz von Open Source

Open Source wird von Teilen der Sicherheitsgemeinschaft als wesentlicher Fortschritt bei der Stärkung des allgemeinen Sicherheitsniveaus angesehen. Da Codes und Methoden öffentlich sind, sollen Fehler oder gar mutwillige Hintertüren zur Schwächung der Sicherheitseigenschaften effektiv vermieden oder zumindest schnell behoben werden. Die Qualität von Open Source Programmen wird jedoch essentiell von der Pflege und dem Know-how der Gemeinschaft bestimmt. Vorkommnisse wie der Heartbleed-Vorfall im Frühjahr 2014 zeigen, dass auch bei Open Source Projekten ein Programm nach mehrmaliger Überprüfung als sicher durch die Gemeinschaft angesehen wurde und sich doch rückwirkend feststellen ließ, dass der Code kritische Fehler enthielt.

- *Die Bundesregierung möge Programme zur Erstellung UND Pflege von Open Source Projekten finanziell unterstützen und dabei gezielt auf die Stärkung der Sicherheitsaspekte achten. Auf diese Weise kann ein nachhaltiges „Community Building" erfolgen.*
- *Denkbar ist die Bereitstellung von Prämienzahlungen für das Auffinden von* Schwachstellen bei Open Source Projekten. Dies setzt Anreize für eine schnelle und wirksame Qualitätssteigerung und vergrößert die Community international.

Führen eines Schnittstellen-Dialogs mit internationalen IKT-Anbietern

IKT-Infrastrukturen sind ein elementarer Bestandteil der Datenschutz- und Sicherheitskette. Sie bilden das Rückgrat der Datenkommunikation, -verarbeitung, und -speicherung. Router, Switches, Access Points und Server sind auf der Hardwareseite ein Ansatzpunkt, um externe Sicherheitskomponenten für Verschlüsselung, Monitoring, Detektion, Identitäten und Authentifizierung – bestenfalls aus einer vertrauenswürdigen Umgebung heraus – einzubringen. Dies muss sicherlich nicht in allen Fällen geschehen, wohl aber leicht möglich sein, wo es das Sicherheitsbedürfnis und/oder das Geschäftsmodell erfordert. Die Möglichkeiten europäischer IKT-Anwender, externe Sicherheitskomponenten mit einem höheren Schutzniveau über Schnittstellen in die IKT-Hardware zu integrieren, sind derzeit kaum gegeben. Standardisierte Schnittstellen erhöhen neben der Sicherheit auch die Chancen, neue Geschäftsmodelle zu kreieren, die ohne Sicherheitskomponenten nicht möglich wären (beispielsweise besserer Service durch gesicherte Fernwartungszugänge). Letztendlich stärkt die Austauschbarkeit die Exportchancen der Unternehmen sowie den Industriestandort Europa insgesamt.

Der ZVEI schlägt vor diesem Hintergrund einen Prozess für einen „Schnittstellen-Dialog“ zwischen europäischen Industrieanwendern und Herstellern von Sicherheitskomponenten sowie internationalen IKT-Infrastrukturanbietern vor:

- *Aufbau des „Schnittstellen-Dialogs“ über die European Cyber Security Organization (ECSO). ECSO ist eine PPP-Plattform zwischen der EU-Kommission, europäischen Industrieanwendern und Security-Anbietern und deckt den notwendigen Teilnehmerzuschnitt im Ansatz bereits ab.*
- *Über ECSO sollte eine Startveranstaltung der genannten Stakeholder auf C-Level stattfinden, die das Anliegen zur Ausarbeitung einer technischen und organisatorischen Roadmap festschreibt und eine Arbeitsstruktur zwischen IKT-Anbietern und -Anwendern beschließt. Zweimal im Jahr wird der Arbeitsfortschritt auf C-Level-Treffen überprüft.*
- *Für den Erfolg der Arbeiten ist ein klares Mandat, umfassende Unterstützung und Nachfassen durch die EU und die Regierungen der Mitgliedstaaten erforderlich.*

Steigerung der KMU-Präsenz in der internationalen Normung

Der Normung und Standardisierung wird berechtigterweise eine strategische Bedeutung zugeschrieben. Dabei bleibt Normung Industrieaufgabe, auch in strategischen Industriebereichen. Gleichzeitig können und sollten Politik und Industrie intensiv zusammenarbeiten.

- *Aufbau einer gemeinsamen Kontaktstelle für das Monitoring sowie die Folgeabschätzung der internationalen Normungsentwicklung im IKT- und Sicherheitsbereich. Vorhandende Stellen, z.B. bei der Bundesnetzagentur, sollten ausgebaut, statt neue andernorts aufgebaut werden.*
- *Sondierung von Möglichkeiten durch Politik und Industrie für eine unabhängige Unterstützung von mittelständischen Unternehmen, damit diese an internationalen Normungsgremien z.B. auf ISO-, IEC-, IETF- oder 3GPP-Level teilnehmen können.*

ZVEI - Zentralverband Elektrotechnik- und Elektronikindustrie e. V.
Fachverband Sicherheit
Lyoner Straße 9
60528 Frankfurt am Main

Ansprechpartner:
Lukas Linke, ZVEI
Telefon: +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org