ZVEI:
Die Elektroindustrie

Positionspapier zum IT-Sicherheitsgesetz

Cyber-Sicherheit als Teil einer strategischen Industriepolitik

Sicherung der Zukunft durch Wettbewerbsfähigkeit und Technologische Souveränität

September 2014

Zentralverband Elektrotechnik- und Elektronikindustrie

Impressum

Cyber-Sicherheit als Teil einer strategischen Industriepolitik
Positionspapier zum IT-Sicherheitsgesetz

Herausgeber:

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

Telefon +49 69 6302-432
Fax: +49 69 6302-322
E-Mail: linke@zvei.org

Verantwortlich:
Lukas Linke

Redaktion:
Arbeitskreis Cyber-Sicherheit

September 2014

Zusammenfassung

Deutsches Know-how ist zu schützen

Wettbewerbsfähige deutsche Unternehmen sind die Fabrikausrüster der Welt. Die Elektroindustrie stellt dafür die Systemintelligenz bereit. Sie nimmt als Querschnittsindustrie an der Schnittstelle zwischen Fabrikhardware (Maschinen und Anlagen) und Unternehmenssoftware (Management) eine Schlüsselrolle ein. Künftig wird die Wettbewerbsfähigkeit der Industrieunternehmen über zwei Faktoren entschieden. Erstens: Über ihre Kompetenz, als Leitanbieter digitale Optimierungsprozesse schnell umzusetzen. Zweitens: Über die Fähigkeit, ihr Know-how effektiv vor Cyberspionage und -kriminalität zu schützen.

Im Zuge der Digitalisierung werden jedoch immer mehr Daten mit verschiedenen Partnern geteilt. Können staatliche und private Akteure sie auslesen oder manipulieren, sind die Unternehmen essentiell bedroht. Als Technologieführer steht die Elektroindustrie dabei im Fokus der Wirtschaftsspionage und Cyberkriminalität. Laut dem amerikanischen Zentrum für strategische und internationale Studien erleidet Deutschland auf diese Weise den größten volkswirtschaftlichen Schaden weltweit.[1] Die Studie beziffert für das Jahr 2013 den Schaden für die gesamte Wirtschaft auf 1,6 Prozent des deutschen BIP, was rund 44 Mrd. Euro jährlich entspricht. Cyber-Sicherheit wird vor diesem Hintergrund zum strategischen Faktor für den Industriestandort Deutschland.

Definition Cyber-Sicherheit

Cyber-Sicherheit umfasst die sichere Verbindung physischer Einheiten (z.B. Maschinen und Steuerungseinheiten) mit dem externen virtuellen Raum, vordergründig dem Internet. Dies betrifft die Datenerzeugung, -übertragung, -speicherung und -auswertung über physische und nicht-physische Schnittstellen. Der Industriekontext bedingt, dass die Industrial-IT-Sicherheit als Teil der Cyber-Sicherheit, die Verfügbarkeit als oberstes Schutzziel festschreibt. Anders als der gebräuchliche IT-Sicherheitsbegriff, verweist der Begriff Cyber-Sicherheit darauf, dass diese innerhalb von Industrieanlagen funktionieren muss, die sowohl virtuellen als auch realen physischen Anforderungen ausgesetzt sind. Durch Wetter, Druck, Temperatur usw. entstehen besondere Herausforderungen für Anlagen und Geräte. Cyber-Sicherheit basiert zudem neben Technik und der generellen Kommunikationsinfrastruktur vor allem auf dem Faktor Mensch. Die von der Bundesregierung angestrebte Technologische Souveränität verfolgt daher das richtige Ziel. Denn künftig lassen sich Wettbewerbsfähigkeit und Technologische Souveränität nicht mehr getrennt betrachten.

Kernanliegen der Elektroindustrie

Ziel der Elektroindustrie ist es, auch in Zukunft als Leitanbieter in Leitmärkten bestehen zu können. Der ZVEI unterbreitet Vorschläge, um durch eine Verbesserung der Cyber-Sicherheit die Wettbewerbsfähigkeit der deutschen Industrie zu sichern. Der ZVEI spricht sich hierbei für technologieoffene Ansätze aus. Die Politik steht dabei in der Verantwortung, Cyber-Sicherheit in Deutschland langfristig weiterzuentwickeln. Dazu zählen der Aufbau des Industrial-IT-Sicherheitssektors als strategische Industrie, die Ergänzung des öffentlichen Beschaffungswesens um das zusätzliche Kriterium „Sicherheit“ sowie die Stärkung des Wirtschaftsschutzes durch praxistaugliche organisatorische, technische und wo notwendig gesetzliche Maßnahmen. Zusammenzuführen sind diese Schritte durch den Beginn eines strategischen Dialogs zwischen Politik und Industrie über die Gestaltung der Technologischen Souveränität.

[1] Center for Strategic and International Studies (2014). Net Losses: Estimating the Global Cost of Cybercrime. Economic impact of cybercrime II.

Politische Grundpositionen

Etablierung, dass Technologische Souveränität im Sinne des Wirtschaftsschutzes die Basis der künftigen Wettbewerbsfähigkeit ist. Daher Aufbau der Industrial-IT-Sicherheitsbranche als strategische Industrie durch:

(1) Aufbau einer strategischen Industrie
- Ergänzung des Beschaffungswesens um das Kriterium „Sicherheit"
- Stärkung der Risikokapitalbasis
- Verbesserung der anwendungsorientierten Forschung und Ausbildung

(2) Etablierung eines Code of Conduct für das Internet der Dinge

(3) Jährliches Treffen zwischen Ministerien und Geschäftsführern der Elektroindustrie

Technologische Souveränität

(1) Klare Positionierung und Einleitung eines strategischen Austauschs
- Realistische Betrachtung und Klärung der Umsetzungsschritte

(2) Verbesserte Kontrollmöglichkeiten entlang der Wertschöpfungskette
- Verbreitung anwendungsorientierter Ende-zu-Ende-Verschlüsselung
- Fertigung sicherheitskritischer Produkte in Deutschland

(3) Stärkung der Kommunikationsinfrastruktur in Deutschland und Europa

(4) Förderung zukunftsgewandter Technologiefelder

IT-Sicherheitsgesetz

(1) Mindeststandards und Meldestellen sind durch die Industriebranchen und -verbände festzulegen

(2) Meldung der Identifikationsmerkmale von Schadprogrammen und Einführung einer Erheblichkeitsschwelle

(3) Klärung der Betroffenheit der Zulieferer: Anlagenbetreiber tragen Hauptverantwortung

(4) Berücksichtigung international praktizierter IT-Standards

(5) Stärkere Berücksichtigung der Technologischen Souveränität

(6) Verlängerung der Umsetzungsfrist auf drei Jahre

(7) Einbeziehung der organisatorischen Dimension

KAPITEL 1: POLITISCHE GRUNDSÄTZE

Elektroindustrie ist Technologieführer in der Industrial-IT

Die Elektroindustrie ist mit rund 840.000 Mitarbeitern die zweitgrößte Industriebranche Deutschlands. In den Bereichen Energietechnik, Medizintechnik, Fahrzeugelektrik, Schienenfahrzeuge, Informations- und Kommunikationstechnik, die anteilig Kritische Infrastrukturen einschließen, erwirtschafteten die ZVEI-Mitgliedsunternehmen im vergangenen Jahr 43,4 Mrd. Euro Umsatz. Weltweit sind die Unternehmen Technologieführer im Bereich der Industrial-IT. Diese ist die Basis der industriellen Vernetzung. Um einzelne Komponenten, Maschinen und ganze Produktionsanlagen zu vernetzen, müssen Mess- und Steuerungseinheiten ihre Leistung ortsunabhängig erbringen und der Datenaustausch muss zum Teil in Millisekunden erfolgen. Dies stellt spezifische Herausforderungen an die Informationstechnik. Angesichts der zahlreichen Programme zur Re-Industrialisierungentstehen globale Marktchancen für deutsche Unternehmen. Kann das Technologie-Know-how jedoch nicht geschützt werden, gefährdet dies den Wirtschaftsstandort Deutschland insgesamt.

Aufbau einer strategischen Industrie

Für die Zukunft ist die sichere Vernetzung in Gesellschaft und Industrie eine strategische Aufgabe. Folglich sind deutsche Unternehmen, die Sicherungslösungen für Datenerzeugung-, -übertragung und -verarbeitung bereitstellen, eine strategische Industrie. Ohne sie ist die deutsche Wettbewerbsfähigkeit schwer zu sichern. Sie entsteht jedoch nicht durch Industrieanstrengung allein, sondern bedarf der Ergänzung des Beschaffungswesens, der Stärkung der Risikokapitalbasis und einer zukunftsgewandten Forschung. Die Politik ist in allen vier Bereichen gefordert.

Aufgrund ihres Erfolgs und Spitzen-Know-hows wurden viele deutsche Unternehmen in den letzten drei Dekaden aufgekauft und in ausländische Konzerne integriert. Auf diese Weise schrumpfte der Anbietermarkt erheblich und es gingen Technologiekenntnisse de facto verloren. Dem sind Marktimpulse entgegenzusetzen, um das Know-how in Deutschland zu erhalten, denn jungen Unternehmen wird die Markteinführung ihrer Produkte durch kostenfixierte, sicherheitsunabhängige Ausschreibungsverfahren erschwert. Um diesen Sektor zu entwickeln, sollte neben der Kostenbetrachtung das **Sicherheitsniveau fester Bestandteil der öffentlichen Beschaffung** sein. Dies verhindert einen nachteiligen Protektionismus, fördert den Wettbewerb und hält Know-how in Deutschland. Internationale Beispiele zeigen, dass die Förderung eines Industriesektors technologisch und fiskalisch eine Win-win-Situation schaffen kann. Dies bedingt, wie oft kritisiert, nicht notwendigerweise die Gründung eines neuen „Sicherheits-Airbus". Die Halbleiter-Initiativen „JESSI" und „MEDEA" zeigten, wie ein wettbewerbsfähiger Industriesektor neu in Deutschland und Europa aufgestellt werden kann.

Neue Ideen benötigen Unterstützung, vor allem in der ersten Umsetzungsphase. Des Weiteren brauchen Sicherheitsinnovationen Risikokapital; das jedoch steht in Deutschland nicht

ausreichend zur Verfügung. Leichter als andere Stellen kann die Politik die **Risikokapitalbasis stärken**. Erfahrungen mit entsprechenden Kreditvergaben, Bürgschaften und Kapitalinstitutionen existieren vielerorts im In- und Ausland. Das Ziel ist eine einfache und schnelle Markteinführung von anwendungsbezogenen Sicherheitslösungen. Auftraggeber, die bereit sind Leuchtturmprojekte auch über längere Zeit umzusetzen, sind ebenso notwendig. Sie fördern die Innovationsfähigkeit in der Industrial-IT Sicherheitsbranche. Gelingt eine bessere Forschung-Markt-Übertragung, kann Deutschland als Leitanbieter für Cyber-Sicherheit seine Position im internationalen Wettbewerb ausbauen.

Weiterer Baustein für die strategische Industrieentwicklung ist eine **zukunftsgewandte und technologieoffene Sicherheitsforschung**. Zu oft basiert die Forschung auf der Absicherung bestehender und damit alter Technologien. Beispielweise lässt sich nicht sagen, ob Router langfristig der Grundstein der Internetkommunikation sein werden. Welche technologischen Rahmenbedingungen wiederum ausschlaggebend für die künftige Sicherheit sein werden, ist daher eine immer dringlichere Fragestellung. Es gilt, öffentliche und private Institute noch stärker darin zu fördern, unabhängig von technischen Pfadabhängigkeiten zu forschen.

Etablierung eines Code of Conduct für das Internet der Dinge

Das Internet der Dinge verändert die Dimensionen sowohl der Datenmenge als auch der rechtlich betroffenen Parteien und Bereiche. Entsprechend ist der vertrauenswürdige Umgang mit Daten die Basis für das Vertrauen in die Unternehmen. Die Elektroindustrie nimmt die Verantwortung für ihre Kunden- und Geschäftsbeziehungen ernst und wird einen Code of Conduct für das Internet der Dinge initiieren. Dieser soll die verantwortungsvolle Nutzung der Daten im Sinne der Datensicherheit und des Datenschutzes auf eine transparente, verlässliche Grundlage stellen. Ziel ist die Wahrung des informellen Selbstbestimmungsrechts in Verbindung mit einer Datennutzung durch die Industrie.

Faktor Mensch berücksichtigen und hochrangigen Austausch einleiten

Cyber-Sicherheit lässt sich nicht einfach kaufen oder allein technisch erreichen. Jedes wirksame Konzept sollte Abläufe, Organisationsstrukturen, Qualifikation, Awareness und Verhaltensweisen berücksichtigen. Zu häufig werden technische Maßnahmen mangels Akzeptanz oder Verständnis nicht berücksichtigt. Dies leistet auch der „Innentäter-Problematik" Vorschub. Effektive Schutzmaßnahmen müssen sich daher nach innen und außen wenden. Klare Zugangs- und Zugriffsregeln sowie eine personell-organisatorische Etablierung der Cyber-Sicherheit auf allen relevanten Ebenen sind wichtige Maßnahmen. Schulungen der Mitarbeiter stärken die Sicherheit genauso wie feste Verantwortliche für die Industrial-IT-Sicherheit in der Produktion. Sicherheitskompetenz entsteht durch Technik und richtiges Verhalten. Aufgabe der Industrie ist es, für die Bedienungsfreundlichkeit der Technik zu sorgen. Gleichzeitig braucht sie die Unterstützung der Politik bei der universitären Ausbildung, der Awareness-Steigerung, bei der Information und Schulung über kriminelle Vorgehensweisen. Ein **jährliches Treffen zwischen Ministerien und Geschäftsführern der Elektroindustrie** zum informellen Austausch über die Lage kann ebenfalls wichtige Impulse geben.

Vernetzung der Industrie ist ohne Cyber-Sicherheit nicht umsetzbar

Wenn im Zuge der Digitalisierung mehr und sensiblere Daten innerhalb und außerhalb der Unternehmen geteilt werden, muss die Datenerzeugung, -übertragung, -speicherung, und -auswertung sowie die verlässliche Datenlöschung abgesichert erfolgen. Die technischen **Interdependenzen steigen**. Die Schwäche eines Bestandteils beeinflusst das gesamte System. Zusätzlich zielt die industrielle Vernetzung darauf ab, dass Fertigungsanlagen bis hin zu einzelnen Komponenten mehr autonome Funktionen übernehmen. Wichtige Entscheidungen finden folglich dezentraler statt. Zwischen Unternehmensmanagement, der einzelnen Maschine, bis hin zum noch zu finalisierenden Produkt ist ein Datenaustausch quer durch die Instanzen vorhanden. Aus linearen Informationsketten **entstehen Informationsnetzwerke**. Im Umkehrschluss erlaubt die Zugriffsmöglichkeit auf einen Teilbereich eventuell den Zugang zum ganzen System. Führt dies zu einem unrechtmäßigen Zugriff auf Produktions-, Kunden- und Forschungsdaten, sind essentielle Unternehmenswerte bedroht.

Cyber-Sicherheit wird somit zum strategischen Faktor. Sie ist nicht länger einzelner Teilbereich einer Wertschöpfungskette oder des Produktlebenszyklus, sondern ein essenzieller Unternehmenswert in allen Bereichen. Cyber-Sicherheit muss künftig als integraler Bestandteil jeder Systemarchitektur und als Bestandteil der Prozesse zur Entwicklung und zum Betreiben von Produkten und Anlagen über die gesamte Lebensdauer betrachtet werden. Sicherheit beginnt damit bereits bei der Produktentwicklung und nicht als nachträgliche Implementierung im Schadensfall. Das bestimmende Prinzip lautet daher „Security by Design".

KAPITEL 2: TECHNOLOGISCHE SOUVERÄNITÄT

Klare Positionierung und Einleitung eines strategischen Austauschs

Der Koalitionsvertrag spricht sich für Maßnahmen zur Rückgewinnung der Technologischen Souveränität Deutschlands und Europas aus. Das ist so dringlich wie wichtig. Auf dem Gebiet der Betriebssysteme, Prozessoren und Netzwerkinfrastruktur besteht für die Industrieunternehmen de facto keine Wahlfreiheit für Produkte aus Deutschland und Europa. Auf Dauer wirken sich Kompetenzlücken in sicherheitsrelevanten Bereichen der Informationstechnologie industriepolitisch nachteilig aus.

Für die Industrie ist eine klare Position der Bundesregierung für eine strategische Kooperation von Politik und Industrie wichtig. Erst dann können Unternehmen Entscheidungen für Forschung und Entwicklung treffen. Kernbereiche und Umsetzungsschritte sollten kooperativ definiert und regelmäßig evaluiert werden. Wichtigste Aufgabe ist es, technologieoffen voranzugehen. Dabei muss die Sicherheitsbetrachtung bewusst über den heutigen Stand der Technik hinausgehen. Die Elektroindustrie strebt dazu einen Austausch mit der Politik an.

Verbesserte Kontrollmöglichkeiten entlang der Wertschöpfungskette

Die derzeitige Herausforderung besteht darin, dass eine sichere Kommunikation über unsichere Netze erfolgen muss. Die weitere Verbreitung verlässlicher und anwendungsorientierter Ende-zu-Ende-Verschlüsselung ist nur ein Sicherheitsbaustein von mehreren. Ebenfalls notwendig sind verbesserte, zuverlässige Kontrollmöglichkeiten über die sicherheitsrelevanten Aspekte der Wertschöpfungskette. Selbst wenn Produkte ihren Verwendungszweck erfüllen, muss weiterhin sichergestellt werden, dass sie keine weiteren sicherheitsrelevanten Merkmale beinhalten. Hersteller und Integratoren benötigen eine Nachvollziehbarkeit der Abläufe ihrer Zulieferer. Eine Anpassung der Audit- und Zertifizierungssysteme sowie ihrer Kriterien ist entsprechend vorzunehmen. Wo dies nicht möglich ist, sollte die Politik dabei unterstützen, langfristig das Know-how zur Veredelung und gegebenenfalls die Fertigung von sicherheitskritischen Produkten in Deutschland anzusiedeln. Ineffiziente Doppelstrukturen sind dabei zu vermeiden.

Stärkung der Kommunikationsinfrastruktur in Deutschland und Europa

Neben der eigenen Fertigungskette steht die Kommunikationsinfrastruktur im Fokus. Den Unternehmen sollte es möglich sein, Informationen über Serverdienste in Deutschland und Europa übertragen, verarbeiten oder speichern zu können. Aus Sicht des ZVEI bestimmen die Rahmenbedingungen, unter denen Produkte und Systeme gefertigt werden, ebenfalls deren Sicherheitslevel. Werden fertigungsrelevante Daten durch eine ungeschützte Datenspeicherung oder Datenübertragung ausgelesen, verlieren die eigentlich verlässlichen Sicherheitseigenschaften der Produkte schnell ihre Wirksamkeit. Im Gegensatz dazu fördert eine vertrauenswürdige und integre Datenspeicherung oder Datenkommunikation das Vertrauen von Unternehmen und Bürgern. Serverstandorte mit transparenten, verlässlichen Bestimmungen zu Cyber-Sicherheit und Datenschutz können sich somit zu einem positiven Marktargument entwickeln. Entsprechend sollten sie auch in Deutschland aufgebaut werden.

Förderung anwendungsbezogener Technologiefelder

Die Stärkung deutscher und europäischer Kompetenzen in der Informationstechnologie sind eine Grundlage für Wachstum und Innovationfähigkeit der deutschen Industrie. Vor diesem Hintergrund spricht sich der ZVEI für eine Förderung anwendungsorientierter Technologiefelder, wie etwa der **Mikroelektronik und Kryptologie**, aus. Flankierend dazu ist eine Anpassung der öffentlichen Beschaffungspraxis, wie oben beschrieben, anzustreben.

KAPITEL 3: IT-SICHERHEITSGESETZ

Gelungene Weiterentwicklung des Gesetzentwurfs

Der ZVEI begrüßt, dass der Gesetzentwurf das Kooperationsprinzip zwischen Politik und Wirtschaft, vor allem in den sensiblen Bereichen bezüglich der Definition von Kritischen Infrastrukturen und IT-Sicherheitsvorfällen, unterstreicht. Ebenfalls ist die differenzierte Meldung von Gefährdungen (anonym) und tatsächlichen Ausfällen (offen) von Infrastrukturen zielführend. Allerdings ist eine strikte Vertraulichkeit nach dem „Need-to-know-Prinzip", sowohl bei Beeinträchtigungen als auch bei Ausfällen, zu gewährleisten. Dies gilt auch für zusammenfassende Berichte des BSI. Die Möglichkeit, dies je nach Branchenentscheidung über eine neutrale Clearingstelle zu tun, erweitert den Handlungsspielraum der Unternehmen in sinnvoller Weise. Angesichts der mehrfachen, massenhaften Kompromittierung von Online-Passwörtern ist die gefundene datenschutzkonforme Prozessregelung sehr hilfreich. Die Hoffnung ist, dass dadurch aufwendige Abstimmungsprozesse zwischen den Behörden verhindert und Unternehmen sowie Bürgern schneller geholfen wird. Zum gleichen Zweck fordert der ZVEI, dass die durch die Bundesregierung angekündigte Kapazitätserhöhung der Behörden, vor allem des Bundesamts für Sicherheit in der Informationstechnik, tatsächlich umgesetzt wird.

Meldung der Identifikationsmerkmale von Schadprogrammen und Einführung einer Erheblichkeitsschwelle

Der § 8b des Gesetzentwurfes sieht vor, dass Unternehmen bei Beeinträchtigungen Informationen zu folgenden Punkten melden: ausgenutzte Sicherheitslücken, gefundene Schadprogramme sowie die eingesetzte und betroffene Informationstechnik auf System- und Komponentenebene. Dieser Umfang führt zu zwei Nachteilen. Erstens drängt die Fülle der geforderten Informationen – selbst bei einer anonymen Meldung – die Unternehmen zu einer umfangreichen Compliance-Prüfung. Das kostet Zeit und erhöht die Rechtsunsicherheit. Zweitens ist das Kriterium „Beeinträchtigung" in § 8b (4) als meldepflichtiges Ereignis zu allgemein. Je nach Auslegung kann darunter nahezu jeder Vorfall subsummiert werden. Es sollte sich zumindest um eine in ihren möglichen Auswirkungen quantitativ und qualitativ erhebliche Beeinträchtigung handeln. Daher ist eine Erheblichkeitsschwelle erforderlich. Drittens erschwert diese statische und hohe Anspruchshaltung den freiwilligen Austausch. Dies ist vor allem hinderlich, wenn ein größeres Unternehmen ein Schadprogramm findet, das bei ihm selbst keinen Schaden verursacht. Das Programm könnte jedoch kleinere, weniger ressourcenreiche Betriebe schädigen. In diesem Szenario ist bereits die einzelne Information benachbarter Unternehmen hinsichtlich der Identifizierungsmerkmale hilfreich. Muss jedoch alles gemeldet werden, könnten Unternehmen von diesem freiwilligen Schritt absehen.

Aus Sicht des ZVEI erscheint eine alternative Betrachtungsweise daher als zielführender. Nicht die genannten Bereiche, sondern die **eindeutigen Identifikationsmerkmale von gefundenen Schadensmerkmalen und Programmen** sollten im Fokus stehen. Die Weitergabe erlaubt es anderen Unternehmen schnell zu prüfen, ob sie ebenfalls betroffen sind. Dies schafft einen

praxistauglichen Mehrwert. Gleichzeitig wird seitens der Politik die Daseinsvorsorge gestärkt und eine erste Basis für das Sicherheitslagebild gegeben.

Klärung der Betroffenheit der Zulieferer:

Anlagenbetreiber tragen Hauptverantwortung

In § 8a des Gesetzentwurfs steht der Satz, dass die Vorgaben nicht nur für Betreiber Kritischer Infrastrukturen gelten, sondern auch für diejenigen, die an diesen Infrastrukturen mitwirken. Dies kann je nach Auslegung 1:1 auf die Zulieferer/Hersteller aus der Elektroindustrie übertragen werden und erhöht die Rechtsunsicherheit bei den Unternehmen. Die Anlagenbetreiber tragen die Hauptverantwortung für die Sicherheit einer Anlage. Die Produkthersteller und Anlagenerrichter haben in ihren Verantwortungsbereichen ebenfalls entsprechende Sicherheitsanstrengungen zu unternehmen. Letztlich hat es aber nur der Anlagenbetreiber in der Hand, das Sicherheitskonzept zu implementieren und über den Lebenszyklus der Anlage aktuell zu halten. Ein Verlagern der Verantwortlichkeiten ist sehr kritisch zu sehen. Im Sinne der Klarstellung sollte der Zusatz bezüglich der Mitwirkung gestrichen werden. Sollte sich der Passus lediglich auf von Betreibern an Dritte ausgelagerte Dienste beziehen, die aber im Sinne des Gesetzes weiterhin im Verantwortungsbereich der Betreiber liegen, ist eine Klarstellung erforderlich. Eine alternative Formulierung könnte lauten: „(…) Infrastrukturen betreibt oder im Zuge einer Dienstauslagerung daran mitwirkt".

Berücksichtigung international praktizierter IT-Standards

Deutschland ist eine Exportnation. Dies bedeutet, dass sich die Kunden der deutschen Industrieunternehmen zum Großteil im Ausland befinden und dort die Rahmenbedingungen für die Verträge gesetzt werden. Deutsche Sonderwege, insbesondere im Sicherheitsbereich, wirken sich somit sehr nachteilig aus und sind unbedingt zu vermeiden. Die Orientierung an international praktizierten IT-Sicherheitsstandards wie der Norm ISO 27001 oder der entstehenden IEC 62443 leistet Abhilfe.

Nutzen bringt dies jedoch nur, wenn die Wahlfreiheit zwischen der Umsetzung nach IT-Grundschutz des BSI oder nach ISO 27001 bzw. IEC 62443 Berücksichtigung findet. Skalierbarkeit, Flexibilität und Staffelbarkeit der Umsetzungsmaßnahmen innerhalb des Zertifizierungsverfahrens gelten als wesentliche Vorteile gegenüber einer Zertifizierung nach IT-Grundschutz. Eine pauschale Festschreibung des IT-Grundschutzstandards wäre vor allem für kleine und mittlere Unternehmen eine Überforderung. Schwer können sie die Ressourcen und Strukturen für ein durchgängiges Informationssicherheitsmanagement oder die Einstellung eines hauptamtlichen Chief-Security, -Compliance oder -Privacy-Officers aufbringen. Wahlfreiheit sollte darüber hinaus die Option beinhalten, dass Betreiber und Zulieferer individuelle Sicherheitsregelungen festlegen können. Die Praxis zeigt, dass vielerorts große OEM-Betriebe eigene Vorgaben mit ihren Zulieferern vereinbaren. Diese privatwirtschaftlichen Regelungen dürfen nicht durch staatliche Mindeststandards gedoppelt werden, der Aufwand für sie darf nicht erhöht werden.

IT-Sicherheit bedingt Stärkung der Technologischen Souveränität

Die Stärkung der Cyber-Sicherheit in Deutschland geht über den Schutz eines störungsfreien Betriebs der Infrastrukturen hinaus. Die Politik trägt zusammen mit der Industrie die Verantwortung, das unrechtmäßige Auslesen von Informationen zu verhindern. Das Know-how der Betreiber und Zulieferer ist zu schützen. Der Umstand, dass dies derzeit im Zuge der Abhängigkeit von ausländischen Betriebssystemen, Netzwerkinfrastrukturen und Prozessoren nur sehr schwer möglich ist, wird nicht adressiert. Neue Technologien in diesen Bereichen werden nicht in Deutschland entwickelt. Dem Ansatz der Technologischen Souveränität ist im Sinne des Wirtschaftsschutzes eine größere Rolle beizumessen.

Längere Umsetzungsfrist

Praxistaugliche Rahmenbedingungen sind ebenfalls maßgeblich. Hierzu hat sich der Bundesverband der Deutschen Industrie (BDI) mit seinem Papier „Erwartungen der deutschen Industrie an ein IT-Sicherheitsgesetz" umfassend positioniert. Der ZVEI unterstützt das darin formulierte Anliegen, die **Umsetzungsfrist des Gesetzes auf drei Jahre** zu verlängern. Je nach individueller Betroffenheit ist eine Vielzahl an zusätzlichen Verpflichtungen zu erfüllen. Betreiber, Integratoren und Zulieferer benötigen ausreichend Zeit, um neue Informationsabläufe, Sicherheitsprozesse und Auditverfahren abzustimmen.

Einbeziehung der organisatorischen Dimension

Das IT-Sicherheitsgesetz konzentriert sich derzeit sehr stark auf die technischen Aspekte, auch wenn es organisatorische Maßnahmen anmahnt. Der Rahmen bleibt zu vage. Das Gesetz suggeriert, dass Cyber-Sicherheit technisch zu lösen sei. Neben der Benennung der 15 Warn- und Meldekontakten sollten die Betreiber Kritischer Infrastrukturen angehalten werden, organisatorische Regelungen und Prozesse innerhalb eines Cyber-Sicherheitsmanagements festzulegen. Eine kontinuierliche Anpassung an Sicherheit als „Moving Target" sollte möglich sein. Dies hat Auswirkungen auf die Cyber-Sicherheitsausbildung in Deutschland. Cyber-Sicherheit kann nicht nur mit Schwerpunkt Netzwerkkommunikation bewerkstelligt werden. Es braucht beispielsweise Sicherheitskenntnisse in der Produktion, der Entwicklung und wahlweise im Vertrieb und Service. Entsprechend sollten Ausbildungs- und Schulungsformate in den Betrieben und an Schulen sowie an Universitäten gefördert werden. Öffentliche Plattformen wie die Allianz für Cyber-Sicherheit können ebenfalls wichtige Angebote geben.

ZVEI - Zentralverband Elektrotechnik-
und Elektronikindustrie e. V.
Lyoner Straße 9
60528 Frankfurt am Main
Telefon: +49 69 6302-0
Fax: +49 69 6302-317
E-Mail: zvei@zvei.org
www.zvei.org