ZVEI: Die Elektroindustrie

Stellungnahme

Nutzen und Grenzen von Zertifizierung und Labels im Kontext Cybersicherheit

Argumente für eine Balance zwischen Kundeninformation & Industrietauglichkeit

Januar 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Zusammenfassung

Die Elektroindustrie bewertet Vorhaben für die Einführung von Zertifizierungs- und Labelsystemen, insbesondere für den B2B-Industriekontext, kritisch. Zum einen lassen sich viele meist durch Verbraucherschutz motivierte Aspekte nicht oder nur eingeschränkt auf den B2B-Bereich übertragen. Zum anderen finden vielerorts bereits Industrieinitiativen zu den Themen Standards und Zertifizierung für Cybersicherheit statt. Die Elektroindustrie schlägt vor, die Industrieinitiativen noch stärker voranzutreiben, ein klar getrenntes Vorgehen bei B2C oder B2B Güter- und Vertragsbeziehungen vorzunehmen und stets auf die tatsächliche Aussagekraft eines angedachten Zertifizierungs- und Labelsystems zu achten. Cybersicherheit wird immer dynamisch sein. Eine statische Zertifizierungs- oder Labelaussage kann unter Umständen den Verbraucherschutz sogar schwächen statt stärken.

Teil 1: Warum die Debatte wichtig ist

Privat- und Industriekunden haben ein verständliches Interesse daran transparent nachvollziehen zu können, mit welchem Grad Hersteller die Cybersicherheit in ihren Produkten berücksichtigt haben. Kunden stellen häufiger die Frage, inwiefern sie Produkten vertrauen können, bevor sie diese in ihr Heim-, Unternehmens- oder Produktionsnetzwerk integrieren. Eine verlässliche und transparente Kundeninformation kann – wenn zielorientiert umgesetzt – einen wertvollen Beitrag leisten.

Die Elektroindustrie liefert qualitativ hochwertige und belastbare Komponenten und intelligente Steuerungssysteme in die ganze Welt. Als Herstellerindustrie ist es seit jeher ihr eigenes Interesse, die Qualität und Sicherheit ihrer Lösungen den Kunden gegenüber transparent darzustellen. Sie sind nicht zuletzt wichtige Marktargumente. Entscheidend ist jedoch, dass die dargestellten Informationen passen, Aussagekraft besitzen, keinem bürokratischen Überbau Vorschub leisten, oder im Kontext von Prüfung und Zertifizierung gar den Industriestandort schwächen. Die Produkt- und Kundeninformation kann auf vielfältige Weise erfolgen. Dies ist gelebte Praxis in der Industrie. Folglich ist eine besonnene Auseinandersetzung mit dem Thema notwendig.

Teil 2: Positionen hinsichtlich Zertifizierung und Labels im Kontext der Cybersicherheit

Für die Erreichung von europaweit einheitlichen und effektiven Maßnahmen zur Stärkungen der Transparenz und Förderung der Cybersicherheit in IoT-Produkten und -Systemen sind aus Sicht der Elektroindustrie folgende Eckpunkte zu berücksichtigen:

- **Gewährleistung der Zukunftssicherheit**: Der technische Fortschritt wirkt sich auch auf Absicherungsmaßnahmen aus. So sind die Anforderungen an die Längen elektronischer Schlüssel über die Jahre

gestiegen. Hard- und Softwarekomponenten müssen diese Entwicklung über Upgrades nachvollziehen können. Ein gestuftes Zertifizierungs- und Labelsystem muss entsprechend bei der Nennung etwaiger Umsetzungsmaßnahmen die Zukunftsfähigkeit berücksichtigen.

- **Gewährleistung der Technologieoffenheit**: Festschreibungen eines bestimmten technischen Standes neigen leicht dazu, de facto Technologien im Hardware- und ggf. Softwarebereich vorzuschreiben. Im Security-Bereich sind Technologien z.T. eng mit konkreten Produkten verbunden, da Nischen- und Spezialanwendungen relativ häufig sind. Ein gestuftes Zertifizierungs- und Labelsystem muss bei der Nennung etwaiger Umsetzungsmaßnahmen allein aus Compliance-Gründen die Technologieoffenheit gewährleisten.

- **Berücksichtigung der internationalen Wettbewerbsfähigkeit**: Entsprechend hilft eine internationale Harmonisierung des Vorgehens dabei, die Wettbewerbsfähigkeit zu erhalten. Sind in ausländischen Märkten andere Anforderungen gegeben, verschlechtert dies die Wettbewerbsfähigkeit deutscher Produkte in technischer oder preislicher Hinsicht.

- **Wandelbarkeit der Cybersicherheit berücksichtigen**: Cybersicherheit ist niemals statisch. Das Schutzniveau sinkt durch den technologischen Fortschritt regulär mit der Zeit. Zudem verändern erkannte Schwachstellen oder neue Angriffsmethoden ad hoc die Sicherheitslage. Insofern läuft ein Zertifizierungssystem, das grundsätzlich lediglich eine Aussage zu einem bestimmten Zeitpunkt X machen kann, stets Gefahr, nicht mehr das tatsächliche Schutzniveau des IoT-Gerätes darzustellen. Im ungünstigsten Fall wird auf diese Weise der Verbraucherschutz durch das Suggerieren eines falschen Schutzniveaus sogar geschwächt, wenn Kunden ihr Verhalten darauf aufbauen. Dies kann dazu führen, dass Kunden einem Label mittelfristig nicht mehr vertrauen und so ein Schaden für betroffene Produkte mit diesem Label entsteht, und dies branchenweit.

- **Anforderungen statt Umsetzungsmaßnahmen vorgeben**: Ideenreichtum und Innovationskraft zeichnen die Herstellerunternehmen seit jeher aus. Sie reagieren täglich auf die sich verändernde Umgebung ihrer Produkte. Entsprechend würde die Vorgabe des technischen Weges bzw. der konkreten technischen Lösung zur Erreichung eines Schutzzieles die Unternehmensfreiheit unverhältnismäßig einschränken sowie über die Zeit qualitativ schlechtere Lösungen hervorbringen. Die Sicherheits- und Bedrohungslage sowie die Möglichkeiten des technischen Fortschritts sind zu dynamisch. Folglich ist es wichtig, den Unternehmen die größtmögliche Flexibilität für die Zielerreichung zu belassen. Dies erreicht man durch eine klare Ziel- aber nicht mit einer Umsetzungsdefinition.

- **Stets sektorspezifisches Vorgehen**: Viele Industriesektoren (z.B. Energie, Gesundheit und Mobilität) haben sehr unterschiedliche Rahmenbedingungen hinsichtlich der Rechtsgrundlagen, Anwendungsszenarien, Kundenwünsche, Technologiereife, der Sicherheits- und Bedrohungslage sowie in Bezug auf den Grad der Vernetzung und

Digitalisierung. Der vermeintlich gemeinsame Nenner der IoT-Definition, „das Gerät ist mit dem Internet vernetzbar“ reicht nicht aus, um ein übergreifendes Zertifizierungs- und Labelsystem sinnvoll anzustreben. Eine Aussage hinsichtlich der verwirklichten Sicherheit bringt dem Kunden ohne eine produktbezogene und anwendungsbezogene Risikoanalyse keinen Mehrwert. Nur ein sektorspezifisches Vorgehen mag die verschiedenen Rahmenbedingungen zielgerecht adressieren.

- **Flexibilität und Wettbewerb über Herstellererklärungen freisetzen**: Cybersicherheit wird im Internet der Dinge flächendeckend zum Einsatz kommen und als Differenzierungsmerkmal dienen. Ein zu enges und statisches Zertifizierungs- und Labelsystem kann die Bandbreite der technischen Security-Lösungen de facto einschränken, insbesondere wenn es nicht nur Anforderungen, sondern Umsetzungsmaßnahmen skizziert. Das behindert Innovationen und die Marktvielfalt. Über Herstellererklärungen können die Unternehmen transparent und vergleichbar darstellen, wie sie die Cybersicherheit in ihren Produkten und Lösungen berücksichtigt bzw. an welchen Standards sie sich orientiert haben. Gegenüber dem Kunden ist hierüber eine differenziertere Aussage zur Sicherheit eines Produktes möglich, als über ein verallgemeinerndes Label, das vielmehr mangels Zukunftsfestigkeit einer Sicherheitsaussage für ein spezifisches Produkt, Gefahr läuft dem Kunden einen falschen Rückschluss über die Sicherheit eines Produktes zu vermitteln.

- **Keine Zertifizierung ohne Standards**: Damit eine Zertifizierung oder ein Label Aussagekraft besitzen, müssen sie auf einem Industriestandard beruhen, der eine einheitliche, vergleichbare, praxistaugliche und technisch erprobte Grundlage schafft. Angesichts der großen Exportorientierung sollten vor allem internationale Standards die Basis sein. Existieren für Sektoren oder IoT-Geräte keine dedizierten Security-Standards oder Regelwerke mit Security-Bezügen, sind diese zu schaffen. Es lassen sich bei engagierter Zusammenarbeit aller interessierten Kreise auch internationale Standards zeitnah bereitstellen. Die Transaktionskosten und Unsicherheiten für ein nicht abgestimmtes, technisch fragwürdiges und ggf. nationales Zertifizierungsvorgehen wären jedoch ungemein größer.

- **Prozesse sind sinnvoller zu zertifizieren als Produkteigenschaften**: Die Wirksamkeit der Sicherheitseigenschaften innerhalb eines IoT-Gerätes ist stets von der Einsatzumgebung des Produktes abhängig (Implementierung, Nutzerverhalten, Vernetzung mit anderen Produkten und Systemen etc.). Entwicklungs-, Produktions- und Qualitäts-managementprozesse in den Unternehmen bleiben im Regelfall gleich bzw. sind sie meist standardisiert, um Effizienz zu schaffen. Gleichzeitig prägen anspruchsvolle Anforderungs-, Entwicklungs-, Produktions- und Testmaßnahmen die Robustheit und Qualität der Systeme und Geräte an sich bzw. schaffen einen Security-Mehrwert für die Entwicklung aber auch für die Bereitstellung von Softwareupdates im Rahmen des Produktlebenszyklus. Insofern bietet es dem Kunden bereits einen Nutzen zu wissen, dass der Hersteller des Gerätes entsprechende branchen- und produktspezifische Prozesse – dargestellt über eine vergleichbare Zertifizierung – implementiert hat.

- **Freiwillige Drittstellenzertifizierung als Grundsatz**: Jede Zertifizierung ist mit z.T. erheblichen Kosten für Hersteller und damit den Endkunden verbunden. Hinzu kommt der Dokumentations- und Zeitaufwand für die Prüfverfahren. Auch die einschlägigen Geschäftsmodelle und -interessen der Unternehmen sind bei der Debatte um ein Zertifizierungs- und Labelsystem zu bedenken. Zu berücksichtigen sind zusätzlich die Dokumentations- und Zeitaufwände anderer regulatorischen Vorgaben (z.B. aus der Funktionalen Sicherheit), die einen z.T. erheblichen Abstimmungsbedarf bedingen. Außer für den (hoheitlichen, militärischen) Hochsicherheitsbereich sollte der Rückgriff auf eine Drittstellenzertifizierung stets die freie Entscheidung des Produktherstellers, in Abhängigkeit von den Kundenwünschen und Marktanforderungen, bleiben. Herstellererklärungen sind zudem ein anerkanntes und erprobtes Mittel, um der Öffentlichkeit dennoch aussagekräftige Informationen zur Verfügung zu stellen.

- **Keine Verkürzung auf Teilaspekte der Security**: Cybersicherheit basiert auf Hardware, Software und Prozessen über den gesamten Lebenszyklus der Systeme und Geräte. Kein Teilaspekt darf den anderen ausspielen. Die besten technischen Vorkehrungen in den Produkten nützen nichts, wenn diese nicht durch entsprechende Implementierung, Nutzung und Verhalten ergänzt werden. Ein Zertifizierungssystem, das bspw. nur die Sicherheitsaspekte der Hardware oder Software verifiziert, verengt den Blick des Kunden und kann bestenfalls nur eine Teilaussage, im ungünstigen Fall gar eine Falschaussage über das Schutzniveau des Gerätes treffen.

- **Konzeptionelle Trennung von Datenschutz und Cybersicherheit**: Häufig werden bei der Diskussion über den Schutz von IoT-Geräten Datenschutz und Cybersicherheit grundsätzlich vermischt. Es wird eine Sicherheitsarchitektur gefordert, die beide Bereiche abdeckt und über ein einheitliches Zertifizierungs- und Labelsystem das jeweilige Schutzniveau ausdrückt. Dies verkennt jedoch die z.T. sehr unterschiedlichen Schutzobjekte (z.B. personenbezogene Daten vs. technische Daten). Darüber bestehen bereits unterschiedlich aufgebauten Rechtsgrundlagen (z.B. Datenschutzgrundverordnung vs. IT-Sicherheitsgesetz und NIS-Richtlinie). So sind die geforderten beiden Schlagworte „Security-by-Design“ und „Privacy-by-Design“ nicht deckungsgleich und über einen Standard oder eine Zertifizierung darzustellen.

- **Keine Orientierung am Energieeffizienz-Label**: Der Stand von Wissenschaft und Forschung zeigt deutlich: Cybersicherheit lässt sich mit gängigen Methoden nicht messen. Die Bedingungen verändern sich zu schnell und können dazu führen, dass bereits in der Zeit zwischen Zertifizierung und Produkteinführungen die Anforderungen nicht mehr erfüllt sind. Bei der Cybersicherheit kommt es im/für das Produkt auf die technischen Eigenschaften, Prozesse, Anwenderkompetenz, Einsatzumgebung und Implementierung im Gesamtsystem gleichermaßen an. Dies unterscheidet die Cybersicherheit deutlich von der Energieeffizienz, die in anschaulicher Weise über ein Ampel-Label auf

einschlägigen Produkten ausgedrückt wird. Aufgrund des bestehenden Konzeptions- und Methodenwiderspruchs lässt sich dieser Ansatz nicht auf die Cybersicherheit übertragen. Um Verwirrung und ggf. Fehlinformationen zu vermeiden, sollten Konzepte für ein Zertifizierungs- und Labelsystem alternative Wege beschreiten.

Teil 3: Handlungsoptionen bei der Gestaltung eines Zertifizierungs- und Labelsystem in der EU

- **Übertragung internationaler Security-Industriestandards unterstützen**: Die internationale Security-Normenreihe IEC 62443 betrachtet bezüglich der Cybersicherheit Anforderungen für technische Aspekte in Produkten (über Security Level), prozess-organisatorische Aspekte in Unternehmen (über Maturity Level) und kombiniert diese zu einem holistischen Ansatz (über Protection Level). Insbesondere wird der oben diskutierte Ansatz über Prozessbetrachtungen statt Produktzertifizierung berücksichtigt. Dieses Vorgehen findet sektorenübergreifend bei vielen Industrieanwendern Akzeptanz und Zustimmung. So ist der Ansatz eventuell auf andere Sektoren übertragbar. Zusätzlich beginnen auch in weiteren Sektoren Arbeiten zu Security-Standards, deren Übertragbarkeit geprüft werden sollte, wie zum Beispiel die ISO AWI 21434 „Road vehicles – Cybersecurity Engineering“. Generell ist es ratsam, die ISO 27001 zur IT-Sicherheit auf ihre Anwendbarkeit im Industriekontext zu prüfen, was der IEC 62443-Standard explizit im Vorwort erwähnt.
  Die EU Kommission möge bestehende Arbeiten zur Übertragung und Implementierung der übergreifenden Security-Standards als Best Practices sondieren und unterstützen.

- **Ansatz über die freiwillige Lightweight-Zertifizierung**: Frankreich bietet über das ANSSI-Zertifizierungssystem einen leichtgewichtigen Ansatz für Bereiche unterhalb des Hochsicherheitsbereiches, der über den Common Criteria Standard abgedeckt wird.
  Die EU Kommission möge die Möglichkeit einer einheitlichen, freiwilligen Übertragung auf die EU-Mitgliedsstaaten prüfen.

- **Definition eines einheitlichen Schemas für Security-Herstellererklärungen**: Das verständliche Anliegen von Zertifizierungs- und Labelsystemen ist es, dem Endanwender klare, vertrauenswürdige und vergleichbare Informationen über ein Produkt oder System zur Verfügung zu stellen. Die gleiche Funktion können auch Herstellerselbsterklärungen übernehmen. Ein derartiges Schema existiert derzeit für Security-Eigenschaften von Produkten und Systemen noch nicht. Dies ließe sich jedoch über die bewährten Normungsprozesse, mandatiert durch die EU Kommission, erzeugen.

Zusammenfassend sollten sich jegliche Betrachtungen zur Cybersicherheit an folgenden Prinzipien orientieren:

1. Risikobasierter Ansatz zur Festlegung der anwendungsorientierten Anforderung
2. Systembezogene Betrachtung, die Hardware, Software und Prozesse einschließt
3. Stets in Bezug auf den jeweiligen Lebenszyklus von Geräten und Systemen

Es ist zu erwarten, dass die aktuellen europäischen Aktivitäten wie AIOTI und ECSO diese Prinzipien aufgreifen werden. Dennoch bleiben die oben beschriebenen Probleme bestehen. Cybersicherheit ist eine gemeinschaftliche Aufgabe von Politik, Industrie, Herstellern und Anwendern. Vor diesem Hintergrund regt der ZVEI dringend die Unterstützung der bestehenden Aktivitäten, mit dem Ziel einer konsensbasierten Lösung, an.

ZVEI: Die Elektroindustrie

Nutzen und Grenzen von Zertifizierung und Labels im Kontext Cybersicherheit

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

Ansprechpartner:
Lukas Linke
Telefon +49 69 6302-432
E-Mail: linke@zvei.org
www.zvei.org

Redaktion:
Arbeitskreis Cybersicherheit

Januar 2017