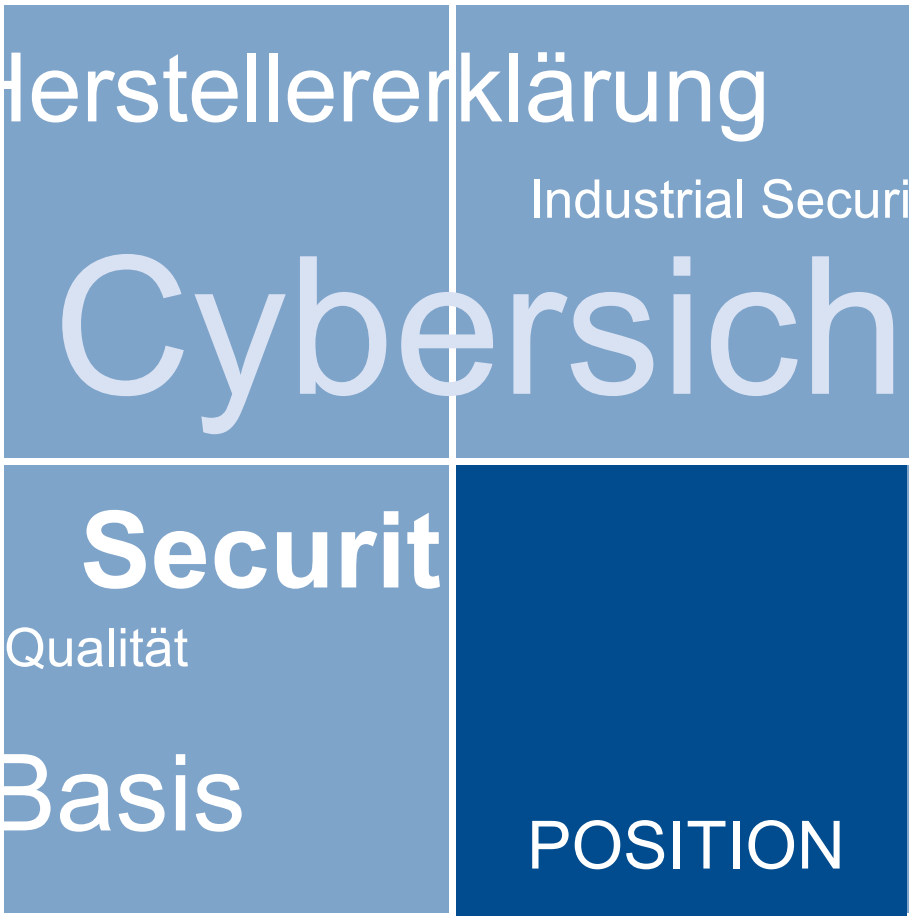
ZVEI: Die Elektroindustrie

Positionspapier

EU Framework for Certification and Labelling

Grenzen und Möglichkeiten der diskutierten Option



September 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Inhalt

Januar 2017

Zentralverband Elektrotechnik- und Elektronikindustrie

Executive Summary

Die Elektroindustrie steht für eine verlässliche und robuste Cybersicherheit in vernetzbaren Geräten. Dies gehört seit jeher zum Selbstverständnis der Branche. Durch die Industrienormung können anpassungsfähige Standards leicht etabliert und die Transparenz gestärkt werden. Die Normung ist daher aus Sicht der ZVEI-Mitgliedsunternehmen der vorrangige Weg, die Ziele der Kommission zu erfüllen. Für den Industriebereich sind Security-Standards wie die IEC 62443 bereits etabliert. Im Konsumgüterbereich sind Initiativen zum Beispiel über das Deutsche Institut für Normung (DIN) angestoßen: „Security by Design Anforderungen für IoT-Geräte im Small Business/Home Umfeld“. Nun kommt es darauf an, die Security-Standards anwendungsspezifisch in den Sektoren weiter voranzubringen.

Das von der EU Kommission angestrebte freiwillige „Framework for Certification and Labelling“ ist vor diesem Hintergrund vor allem auf europäischen und internationalen Security-Standards aufzubauen. Für die Bereiche, in denen noch keine Standards bestehen, skizziert das vorliegende Positionspapier Vorschläge für Basis-Anforderungen sowie einen Definitionsansatz für vernetzbare Geräte über die IP-Schnittstelle. Die Punkte stellen sicher, dass die Anwender und Hersteller die Anforderungen erfüllen können, die Komplexität der IoT-Welt reduziert wird und eine internationale Kompatibilität gewährleistet ist. Unser gemeinsames Ziel ist die Stärkung des europäischen digitalen Binnenmarktes. Ohne einheitliche Anforderungen sind die Digitalisierung sowie der digitale Binnenmarkt nicht zu realisieren.

Die ZVEI-Mitgliedsunternehmen nehmen aufmerksam zur Kenntnis, dass ein möglicher Regulierungsbedarf durch die Kommission geprüft werden soll. Für die Anwendungsbereiche, für die sich tatsächlich ein Regelungsbedarf begründen lässt, sollte das New Legislative Framework (NLF) als Rahmen gesetzt werden. Das NLF bietet über das Modul A den geeignetsten Weg, eine schnelle und anpassungsfähige Umsetzung der Richtlinie zu gewährleisten. Für diesen Fall formuliert das Positionspapier Vorschläge zur Ausgestaltung der Elektroindustrie. Für einen Dialog dazu stehen die ZVEI-Mitglieder gerne bereit.

1. Cybersicherheit gehört zum Selbstverständnis der Branche

Die Elektroindustrie ist Rückgrat und Hersteller der Digitalisierung zugleich. Ihre Produkte kommen in allen relevanten Gesellschafts- und Wirtschaftsbereichen zum Einsatz: Von Consumer Electronics, Smart Home & Smart Building und Industrieausrüstung bis hin zu (Elektro-) Mobilität, Energie und Gesundheit. Die 1.600 ZVEI-Mitgliedsunternehmen sind im Konsum- und Industriegüterbereich Know-how-Führer, zum Beispiel für integrierte Software in Geräten und Komponenten (z.B. Smart-TV, Haushaltsgeräte, Videokameras, Medizingeräte und Industriesteuerungen). Aspekte der Cybersicherheit und IT-Regulierung betreffen daher die Elektroindustrie unmittelbar.

Vor diesem Hintergrund liegt die Stärkung der Cybersicherheit (engl. Security) im Eigeninteresse der Elektroindustrie. Ohne den Schutz von personenbezogenen und technischen Daten sind die Vorteile der Digitalisierung nicht zu realisieren. Unsere Kunden sollen stets sicher ihre Geräte und Apps verwenden können. Industriemechaniker können über gesicherte Kommunikationswege weltweit auf Maschinen aus der Ferne zugreifen, ohne dass Reisen notwendig werden. Unmittelbar wirken sich Security-Vorfälle negativ auf das Vertrauen der Kunden und die Markenwahrnehmung aus. Daher entspricht es dem Qualitätsverständnis der ZVEI-Mitglieder, Security-by-Design kontinuierlich weiterzuentwickeln. Wir sind von der steigenden Bedeutung der Cybersicherheit für Verbraucherschutz, Produktqualität und Kundenbindung überzeugt. Ausdruck findet dieses Selbstverständnis in der Normung. Zahlreiche Security-Standards bestehen bereits. Über 800 Richtlinien und Standards wurden inzwischen von der Industrie und weiteren Stakeholdern erarbeitet (siehe Abschnitt 2.7.).

2. ZVEI-Positionen und -Empfehlungen

Für die Ausgestaltung des freiwilligen EU Framework bringen die ZVEI-Mitgliedsunternehmen nachfolgende Punkte in die Diskussion ein. Wichtigstes Ziel muss es sein, die Cybersicherheit für alle Betroffenen sowie die Wettbewerbsfähigkeit der europäischen Industrie gleichermaßen zu stärken.

2.1. Auswahlkriterien für Anforderungen

Es gibt allgemeine Prinzipien, die bei der Auswahl der Anforderungen eine Rolle spielen sollten, um die Praxistauglichkeit zu gewährleisten. Die Anforderungen sollten sich an dem etablierten „SMERC“-Prinzip orientieren:

- **Specific** – Anforderungen müssen anwendungsspezifisch betrachtet werden.
- **Measurability** – Anforderung muss eindeutig bestimmbar bzw. nachprüfbar sein.
- **Enforceability** – Anforderungen müssen durch die Marktüberwachung durchsetzbar sein.
- **Relevance** – Anforderungen müssen relevant für die Security und Anwender sein.
- **Competition friendly** – Es darf keine nennenswerten nachteiligen Auswirkungen auf die Wettbewerbsfähigkeit der Industrie geben.

Die Kriterien stellen sicher, dass die Anforderungen zu den Fähigkeiten der Produkte und Prozessen passen. Darüber hinaus sind sie für die Industrie maßgeblich, um eine konkrete und zeitnahe Umsetzung zu gewährleisten, die gleichzeitig im Sinne eines Level Playing Field für alle Akteure gemeinsam gelten. Zudem wird sichergestellt, dass eine Anpassung jederzeit möglich ist, was angesichts der Komplexität und Dynamik der IoT-Welt dringend geboten ist.

2.2. Basis-Anforderungen

Es ist eindeutig, dass die Security-Anforderungen in den einzelnen Produktgruppen und Sektoren differenziert betrachtet werden müssen. Dennoch lassen sich wahrscheinlich gemeinsame Ansätze definieren. Die ZVEI-Mitgliedsunternehmen bringen auf Basis des „SMERC-Prinzips“ folgende Punkte in die inhaltliche Diskussion ein:

1. Die Pflege von Software durch Security relevante Updates wird für klar definierte und kommunizierte Zeiträume durch den Hersteller umgesetzt. Bekannte oder neu erkannte Schwachstellen können damit zeitnah geschlossen werden. Betreibt der Anwender darüber hinaus das vernetzbare Gerät, ist er für die Absicherung verantwortlich. Angesichts der unterschiedlichen Innovations- und Produktzyklen im Konsum- und Industriegüterbereich (Spanne: wenige Monaten bis mehrere Jahrzehnte) lassen sich keine einheitlichen Fristen festlegen. Die Bestimmung muss daher in enger Abstimmung mit allen Betroffenen auf Basis der Erfahrungswerte in den Sektoren erfolgen.

2. Falls ein Schließen von Schwachstellen, besonders für ältere Geräte, nicht möglich ist, stellt der Hersteller Alternativmethoden bereit (z.B. Abschalten einzelner Dienste). Über die Auswirkungen dieser Alternativen wird der Kunde informiert, so dass er eine risikobewusste Entscheidung treffen kann.
3. Vernetzbare Geräte bieten eine anwendungsspezifische und überprüfbare Basis-Cybersicherheit, die sich an der vorgesehenen Verwendung und Betriebsumgebung ausrichtet. Vorschlag:
    a. Authentifizierung
    b. Rollen- und Rechtemanagement
    c. Kommunikations-Sicherheit
    d. Maßnahmen für den Integritätsschutz (Daten, Systeme und Prozesse)
    e. Update-Fähigkeit der Geräte

Selbstverständlich werden darüber hinaus alle regulatorischen Vorgaben zum Beispiel für die funktionale Sicherheit und den Datenschutz auf Produkt- und Prozessebene von den Herstellern umgesetzt. Daher finden sie in der Auflistung keine extra Erläuterung.

2.3. Definition des Anwendungsbereichs über IP-Schnittstelle

Was ist ein vernetzbares Gerät? Die aktuelle Schnelldefinition „Jedes Gerät, das mit dem Internet vernetzbar ist“ hilft nicht weiter. Der ZVEI schlägt eine anfängliche Begriffsbestimmung auf funktionaler Basis vor. Vernetzbare Geräte verfügen über eine IP-Schnittstelle nach außen. Sie werden direkt oder über eine Punkt-zu-Punkt-Verbindung (z.B. via Router oder Mobiltelefon) mit dem Internet verbunden. Sicherlich bestehen noch viele weitere Kommunikationsstandards, die die IoT-Welt prägen. Hilfreich wird jedoch sein, mit einem Kernbereich zu beginnen und je nach Bedarf den Anwendungsbereich begründet zu erweitern.

2.4. „New Legislative Framework“ als zentraler Prozess

Die Entwicklungsdynamik im Bereich der Cybersicherheit ist hoch. Angriffsmethoden und adäquate Schutzmaßnehmen passen sich fortwährend an. Keine Regulierung kann für diese Rahmenbedingungen ein statisches, festgeschriebenes Set an Security-Anforderungen definieren. Innerhalb weniger Monate würde sie jede Wirksamkeit verlieren und sich zum erheblichen Wettbewerbsnachteil für europäische Unternehmen entwickeln – insbesondere dann, wenn konkrete Umsetzungsmaßnahmen in der Richtlinie festgeschrieben werden. Für die Anwendungsbereiche, für die sich tatsächlich ein Regelungsbedarf

begründen lässt, sollte das New Legislative Framework (NLF) als Rahmen gesetzt werden.

Das NLF stellt sicher, dass die Anforderungen zu den Fähigkeiten der Produkte passen. Die Definition erfordert einen kartellrechtlich konformen Prozess. Einzelne Akteure, seien es Plattformen, Agenturen oder Konsortien, können dies nicht leisten. Die europäischen Normungsorganisationen gewährleisten zudem wichtige Prinzipien, die für den Erfolg und die Praxistauglichkeit der Richtlinie maßgeblich sind:

- Einheitlichkeit und internationale Kompatibilität der Ergebnisse
- hohe Anpassungsfähigkeit: kontinuierliche Einbeziehung der technischen Entwicklung leicht möglich
- hohe Akzeptanz der Industrie
- Abdeckung aller relevanten Sichtweisen (Verbraucher, Behörden, Unternehmen) und Marktrollen (Hersteller, Integratoren, Installateure, Betreiber)

2.5. Modul A (Herstellerselbsterklärung) als Konformitätsbewertung

Die EU-Richtlinien sehen verschiedene Verfahren vor, damit Unternehmen die Einhaltung der Anforderungen bzw. ihre Konformität mit den zugrundeliegenden harmonisierten Normen erklären können.[1] Über das Modul A (Herstellerselbsterklärung) können Unternehmen flexibel auf eine Änderung der Anforderungen und Normen reagieren. So entstehen im Vergleich zu anderen Modulen geringere Kosten und Zeitverzögerungen, da diese eine Drittstelle verbindlich vorsehen.

Eine verpflichtende Drittstellenzertifizierung zur Konformitätsbewertung lehnen die ZVEI-Mitgliedsunternehmen entschieden ab. Sie stellt außerhalb der Kritischen Infrastrukturen einen unverhältnismäßigen Eingriff in die Privatautonomie der Unternehmen dar. Zudem birgt sie keinerlei Vorteile hinsichtlich der Security-Qualität der Produkte oder Rechtssicherheit für die Unternehmen. Herstellerselbsterklärungen stärken im gleichen Maße die Transparenz und Verbindlichkeit. Es gehört zum Selbstverständnis der Unternehmen, dass alle Angaben vollständig und korrekt aufgeführt werden. Die Marktüberwachung trägt dafür Sorge. So enthält eine Zertifizierung gegenüber der Herstellerselbsterklärung keinerlei Security-Vorteile für den Anwender.

[1] siehe Beschluss 768/2008/EG

2.6. Normungsmandat an CEN/Cenelec

Zusammen mit anderen Anwenderbranchen wie dem Maschinenbau fördert die Elektroindustrie seit jeher die europäische Normung bei CEN/Cenelec. Sie verbinden die maschinelle und elektrotechnische Normung mit den Themen der Digitalisierung und Cybersicherheit.[2] Kennzeichnend für die erfolgreiche Arbeit ist die hohe Akzeptanz der Ergebnisse seitens der Industrieanwender von Cybersicherheit und konsensorientierte Meinungsbildung nach dem „Ein Vertreter, eine Stimme"-Prinzip. Über diesen Weg wird die Rolle von mittelständischen Unternehmen gestärkt. Der ZVEI spricht sich daher klar für die Vergabe des NLF-Normungsmandates an CEN/Cenelec aus.

2.7. Berücksichtigung bestehender Security-Standards

Ein sektorales, schrittweises Vorgehen ist dringend geboten. Existieren in einem Anwendungsbereich zum Beispiel Security-Normen, Betreiberkonzepte oder die Möglichkeit zur Realisierung von Schutzzonen, besteht kein gesetzlicher Regelungsbedarf. Es bestehen zahlreiche Security-Standards bzw. befinden sie sich in Bearbeitung. Der Security-Navigator der Deutschen Kommission Elektrotechnik Elektronik Informationstechnik (DKE) listet 819 existierende Richtlinien und Standards für Cybersicherheit auf.[3] Die Cyber Security Coordination Group (CSCG) skizziert zusammen mit der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) in einem Whitepaper ebenfalls die bereits etablierten Normen auf.[4] Darüber hinaus ist Cybersicherheit auch international gesetzt:

- Im Industriebereich nimmt die internationale Norm IEC 62443 eine zentrale Stellung ein. Sie definiert abgestufte Security-Anforderungen für Produkte und Prozesse und dies für alle Beteiligten: Hersteller, Integratoren und Betreiber. Andere Sektoren beginnen bereits, diese Inhalte für ihren Bereich zu übertragen.

[2] siehe CEN-CLC Focus Group on Cybersecurity
siehe CEN/CLC/TC 13 Cybersecurity and Data Protection
siehe CEN/CLC/TC 8 Privacy management in products and services
siehe IEC/TC 65 WG 10 Security for industrial process measurement and control
[3] siehe Link: https://www.security-standards.de/ITSecurityGrid.html (abgerufen am 09.08.17)
[4] siehe Link: http://www.din.de/blob/61520/377b6def0b8679a61c0252b5d1930c52/cscg-white-paper-data.pdf (abgerufen 11.08.17) und Link: https://www.enisa.europa.eu/publications/gaps-eu-standardisation (abgerufen 11.08.17)

- Auch im Automobilbereich haben seit einiger Zeit die Arbeiten zur Cybersicherheit begonnen. Als Beispiel ist hier das Projekt der ISO/TC22 „Automotive Security“ zu nennen.
- In Deutschland treibt das Deutsche Institut für Normung (DIN) über die Projekte „IoT Security“ und „Sichere Identitäten“ die Arbeiten im Konsumgüter- und Industriebereich voran.

Die EU Kommission trägt vor diesem Hintergrund die wichtige Verantwortung:

1. Für den jeweiligen Anwendungsbereich des EU Framework sind bestehende Security-Inhalte aufzunehmen und zu berücksichtigen. Es dürfen keine doppelten oder gar widersprüchlichen Anforderungen gestellt werden.
2. Eine Analyse für die europäische Ebene durchzuführen, um zu identifizieren, wo wirklich noch Security-Inhalte fehlen. Zahlreiche Organisationen haben hier Vorarbeiten geleistet.[5]

Auf diese Weise können mögliche Ineffizienzen und Dopplungen effektiv vermieden werden. Der ZVEI stellt gerne Input für die Bedarfsanalyse bereit.

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

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

September 2017

[5] Zu nennen ist die Cybersecurity Coordination Group (CSCG) bei CEN/CENELEC sowie die WG 1 der European Cybersecurity Orgnisation (ECSO).