Cybersecurity in der Schweiz – quo vadis?

Die Bedeutung der Normen | Was können wir für die Cybersicherheit von der sicheren Erzeugung und Anwendung von Elektrizität lernen? Welche Rahmenbedingungen sind nötig und wo steht die Schweiz diesbezüglich? Was kommt auf Unternehmen zu? Ein Blick auf Fehlentwicklungen und Chancen.

LEVENTE DOBSZAY

Die «digitale Welt» entwickelt sich schneller als alles Bisherige in der Menschheitsgeschichte. Ebenso rasant nehmen die Probleme wegen fehlender Cybersicherheit zu. Im «digitalen Wilden Westen» kann heute immer noch jeder weitgehend ungehindert unsichere vernetzte Produkte und Internetdienste auf den Markt bringen. Trotzdem wird von der Anwenderseite erwartet, diese sicher zu nutzen. Diesen Sachverhalt könnte man als Cybersicherheits-Paradoxon bezeichnen.

Da bisher weder die Hersteller und Dienstanbieter noch die Anwender wirksame Sicherheitsstandards etablieren konnten, muss von einem Marktversagen hinsichtlich der Cybersicherheit gesprochen werden. Als Ursachen können fehlende Sicherheitsvorschriften, mangelndes Sicherheitsbewusstsein, fehlendes Fachwissen, asymmetrische Kräfteverhältnisse und ökonomische Fehlanreize identifiziert werden. Dieser Fehlentwicklung der letzten Jahrzehnte gilt es, entschlossen und gezielt entgegenzuwirken, um das Vertrauen wiederherzustellen, die Risikokosten tragbar zu machen und ein Fundament für eine sichere Digitalisierung zu legen. Cybersicherheit braucht sichere Produkte, die sicher genutzt werden. Dazu müssen sich sowohl die Hersteller und Anbieter als auch die Anwender an grundlegende Sicherheitsstandards halten. Der Gesetzgeber steht in der Pflicht, die notwendigen gesetzlichen Rahmenbedingungen dafür zu schaffen und die Sicherheit auf beiden Seiten einzufordern.

Lehren aus der Elektrifizierung

In der Elektrotechnik sorgen Gesetze und Normen schon lange für Sicherheit, und ihre Einhaltung wird systematisch überprüft. Vor über 100 Jahren war die Elektrifizierung das, was heute die Digitalisierung ist. Der Umgang mit Elektrizität war damals «komplex» und sogar lebensgefährlich. Die biophysikalischen Vorgänge bei einem Stromschlag waren noch nicht so erforscht und bekannt wie heute. Die sichere Bedienung der damals noch oft lebensgefährlichen Produkte war ähnlich anspruchsvoll wie heute die sichere Nutzung vernetzter Hardware und Software.

Wie würden Sie heute die Sicherheit der Toaster vor 100 Jahren beurteilen?

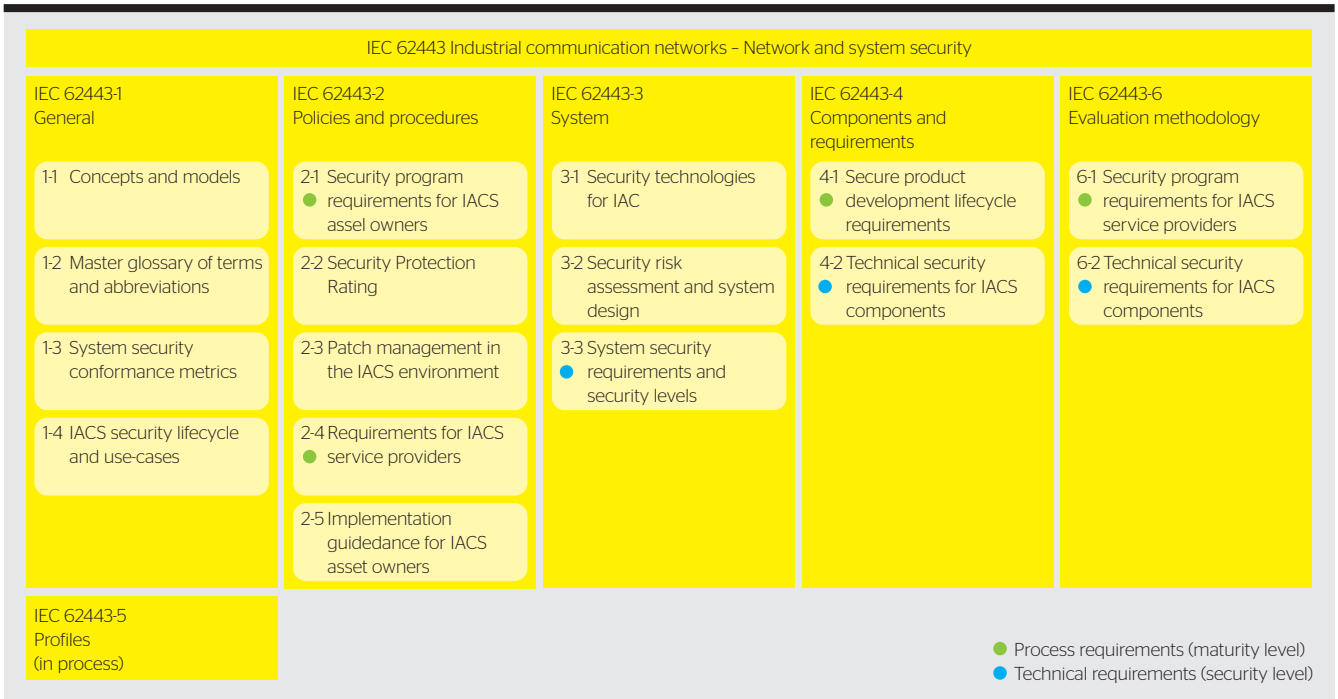
Bild: Levente Dobszay, Pixabay

Der Schweizerische Elektrotechnische Verein (SEV) – die heutige Electrosuisse – hat 1896 die ersten Sicherheitsvorschriften für den Bau und Betrieb von Starkstromanlagen vorgelegt. Seit dem Bundesgesetz betreffend elektrischer Schwach- und Starkstromanlagen von 1902 wurde viel für die Verbesserung der Sicherheit getan. Heute verweist die Niederspannungs-Installationsverordnung (NIV) zur Umsetzung des Elektrizitätsgesetzes (EleG) auf «anerkannte Regeln der Technik». Solche harmonisierten Sicherheitsstandards bestehen mit den Normen der internationalen elektrotechnischen Kommission (IEC) auf globaler Ebene und des Europäischen Komitees für elektrotechnische Normung (Cenelec) auf europäischer Ebene. Diese werden durch die Schweizer Niederspannungs-Installationsnorm (NIN) als anwendungsorientierte Umsetzungsnorm ergänzt. Mit den Bundesgesetzen über die Produktesicherheit und die Produktehaftung besteht in der Schweiz auch für die Sicherheit elektrotechnischer Geräte eine Gesetzesgrundlage im Einklang mit der EU-Richtlinie 2001/95/EG über die allgemeine Produktsicherheit.

Heute ist der Umgang mit Elektrizität dank Sicherheitsvorschriften und -standards weit weniger gefährlich als noch vor 100 Jahren. Es würde sich anerbieten, die Erfolgsgeschichte der elektrischen Sicherheit für die Cybersicherheit in einer der digitalen Welt angepassten Weise zu wiederholen.

Verpflichtende Sicherheitsstandards

Regulatorien, um dem herrschenden Cybersicherheitsdesaster Abhilfe zu schaffen, sind weltweit in Entstehung.



Aufbau der Normenreihe IEC 62443.

Doch während die Regulierungsaktivitäten in der EU schon fortgeschritten sind, wurde in der Schweiz bisher lediglich das Datenschutzgesetz an die Datenschutzgrundverordnung (DSGVO) der EU angepasst.

Nicht zuletzt soll in der EU mit dem «Cyber Resilience Act» (CRA) [1], der im September 2022 als Entwurf publiziert wurde, die Erfüllung definierter Sicherheitsanforderungen für Hardware- und Software-Produkte, die mit dem Internet verbunden sind, über deren «gesamten Lebenszyklus» und auf jeder Stufe der Wertschöpfungskette als Marktzulassungsbedingung festgeschrieben werden. Von Herstellern und Anbietern werden entsprechende Sorgfaltspflichten eingefordert. Die Anforderungen für die CE-Kennzeichnung sollen entsprechend erweitert werden, damit sich Kunden und Unternehmen auf die Cybersicherheit der CE-gekennzeichneten Produkte verlassen können. Mit dem CRA würden auch Meldepflichten und der Nachweis von Mindestanforderungen verpflichtend, die derzeit noch freiwillig sind.

Auch wenn die EU-Regulatorien im Detail noch einzelne Unzulänglichkeiten aufweisen, geben sie eine klare Stossrichtung vor und läuten das Ende des digitalen Wilden Westens ein. «Security by Design and by Default» wird in absehbarer Zeit von einer Idee zu einem einklagbaren Recht.

Obwohl die Schweiz bislang stets unter den Pionieren bei der Festlegung von Sicherheitsstandards war, gehört sie aktuell zu den Ländern mit den wenigsten Rechtsgrundlagen für die Cybersicherheit. In der Schweiz besteht weder eine gesetzliche Pflicht zur Anwendung technischer Sicherheitsnormen, noch bestehen gesetzliche Anforderungen an diese. Im Vergleich zur EU hat die Schweiz diesbezüglich einen Rückstand von zehn Jahren aufzuholen und läuft zurzeit Gefahr, den Anschluss zu verlieren. Wird dies verschlafen, bleibt nichts anderes übrig, als die bürokratischen Vorschriften der EU zu übernehmen, wobei eine schlanke Schweizer Lösung, die mit den EU-Regulatorien harmonisiert ist, vorzuziehen wäre. Nur leider scheint sich in der Schweiz niemand dafür zuständig zu fühlen.

Was kommt auf die Unternehmen zu?

Unternehmen werden es als Anwender einfacher haben, vernetzte informationstechnische Systeme sicher zu nutzen und zu betreiben, wenn diese sicherer werden. Ihnen bleibt aber auch dann noch genug zu tun, um ihre «digitale Überlebensfähigkeit» sicherzustellen. Dazu können sie sich an bestehenden Standards wie der ISO/IEC 27000-er Normenreihe oder dem auf dem NIST Cybersecurity Framework basierenden IKT-Minimalstandard orientieren.

Besonders Hersteller, die vernetzte digitale Komponenten in ihren Produkten verbauen, und Dienstleister, die solche Produkte bei ihren Kunden integrieren, sollten sich rechtzeitig auf die Regulierung der digitalen Welt vorbereiten, um nicht plötzlich überrascht zu werden. Für Hersteller wichtig zu wissen ist vor allem, welche Anforderungen sie künftig für eine CE-Konformität ihrer vernetzten Produkte erfüllen müssen. Eine Übersicht dazu bietet das Factsheet zum Cyber Resilience Act [2]. Für die Umsetzung ist insbesondere die Normenreihe IEC 62443 massgebend, die sich im Gegensatz zur ISO/IEC 27000-er Normenreihe nicht nur an Anwender richtet, sondern Hersteller, Integratoren und Betreiber gleichermassen adressiert.

Normenarbeit für die Cybersicherheit

Der strategischen Bedeutung der Standardisierung im IT-Bereich wird in der Schweiz zu wenig Gewicht beigemessen. Technische Normen werden in der Schweiz auf freiwilliger, unentgeltlicher Basis durch engagierte Fachspezialisten als Mitglied in einer Normenorganisation erarbeitet und mitgestaltet. Entsprechend sind Ergebnisse

Bild: IEC 62443, InfoGuard AG

bezüglich Inhalt, Qualität und Fertigstellungstermin oft schlecht voraussagbar. Inhaltliche Mitbestimmung, Wissensvorsprung oder ein Ertrag seitens der Normenorganisation durch den Normenverkauf sind die Motivationsfaktoren für die Normenarbeit. Die Mitarbeit setzt in der Regel die kostenpflichtige Mitgliedschaft in einer Normenorganisation voraus. Normenarbeit ist deshalb für hochqualifizierte Fachkräfte wenig attraktiv, wenn sie nicht von ihrem Arbeitgeber mit der Wahrnehmung von Unternehmensinteressen bei der Normung beauftragt werden. Den sich mit Cybersicherheit beschäftigenden Normungsgremien der Schweiz fehlen daher die nötigen Ressourcen, um sich bei allen wichtigen Themen bei der Normenerarbeitung einzubringen, Dokumente aus übergeordneten europäischen und internationalen Gremien zu bearbeiten und zu diesen Stellung zu beziehen.

Es wäre begrüssenswert, wenn sich Unternehmen stärker bei der Erarbeitung der Normen für die Cybersicherheit engagieren würden, um Schweizer Interessen über die nationalen Normungsorganisationen in die europäischen und internationalen Normungsgremien einzubringen und sicherzustellen. Dafür muss Normenarbeit durch eine Ausgestaltung von Anreizmodellen für Experten besser entlohnt und gefördert werden, damit möglichst viel vorhandene Expertise eingebracht werden kann und Normen mitgestaltet werden können. Nicht zuletzt wäre es angebracht, dafür Fördergelder bereitzustellen, um damit den Wirtschaftsstandort Schweiz zu stärken und einen wertvollen Beitrag zu leisten, damit Hard- und Software künftig ebenso sicher sind wie Toaster.

Referenzen
[1] digital-strategy.ec.europa.eu/en/policies/cyber-resilience-act
[2] digital-strategy.ec.europa.eu/en/library/cyber-resilience-act-factsheet

Autor
Levente J. Dobszay ist Senior Cyber Security Consultant bei InfoGuard.
→ InfoGuard AG, 6340 Baar
→ levente.dobszay@infoguard.ch

Normenentwürfe und Normen

Bekanntgabe

Im Entwurfsportal der Switec (www.switec.info/de/entwurfsportal, alternativ www.switec.info) finden Sie alle zur Kritik vorgelegten Entwürfe, das nationale Arbeitsprogramm sowie Informationen über das schweizerische technische Regelwerk.

Stellungnahme

Im Hinblick auf die zukünftige Übernahme in das schweizerische technische Regelwerk werden Entwürfe zur Kritik ausgeschrieben. Alle interessierten Kreise sind eingeladen, diese Entwürfe zu prüfen und Stellungnahmen fristgerecht sowie schriftlich an folgende Adresse einzureichen: Electrosuisse, CES, Luppmenstrasse 1, CH-8320 Fehraltorf, bzw. ces@electrosuisse.ch.

Erwerb

Entwürfe (im Normenshop nicht aufgeführt) und/oder zurückgezogene Normungsdokumente können, gegen eine Kostenbeteiligung, bei Electrosuisse, Normenverkauf, Luppmenstrasse 1, CH-8320 Fehraltorf, Tel. +41 58 595 11 90, bzw. normenverkauf@electrosuisse.ch bezogen werden.

Weitere Informationen über SN-, EN und IEC-Normdokumente gibt es unter shop.electrosuisse.ch/de/normen-und-produkte/normen, wo auch alle geltenden Normungsdokumente der Elektrotechnik erworben werden können.

Projets et normes

Annonce

Sur le portail de projets nationaux Switec (www.switec.info/fr/portail-de-projets-nationaux, resp. www.switec.info/fr), vous trouverez tous les projets de normes mis à l'enquête, le programme de travail national ainsi que des informations sur les règles techniques suisses.

Avis

En vue d'une future reprise dans les règles techniques suisses, les projets de normes sont soumis à la critique. Toutes les parties intéressées sont invitées à examiner ces projets et à soumettre leurs avis dans les délais fixés ainsi que par écrit à l'adresse suivante : Electrosuisse, CES, Luppmenstrasse 1, CH-8320 Fehraltorf, resp. ces@electrosuisse.ch.

Achat

Les projets soumis (non répertoriés dans la rubrique Normes du shop) et/ou les documents de normalisation retirés peuvent être obtenus, moyennant une participation aux frais, auprès d'Electrosuisse, Normenverkauf, Luppmenstrasse 1, CH-8320 Fehraltorf, tél. +41 58 595 11 90, resp. à l'adresse électronique suivante : normenverkauf@electrosuisse.ch. De plus amples informations à propos des documents normatifs SN, EN et IEC sont disponibles sur le site shop.electrosuisse.ch/fr/normes-et-produits/normes, où tous les documents normatifs en vigueur du secteur de l'électrotechnique peuvent aussi être acquis.