Kein Produkt mehr ohne Cybersecurity

Keywords
- *Cybersecurity*
- *Cyber Resilience Act (CRA)*
- *Anlagensicherheit*

Der Cyber Resilience Act macht Cybersecurity für Hersteller zur Pflicht – und hilft damit auch Betreibern

Der Cyber Resilience Act (CRA)[1] markiert einen bedeutenden Fortschritt in der Regulierung der Cybersicherheit und wurde am 10. Oktober vom Europäischen Rat verabschiedet. Diese weltweit erste Verordnung ihrer Art wird noch in diesem Jahr in Kraft treten und gilt unmittelbar in allen EU-Mitgliedstaaten. Sie verlangt von Herstellern innerhalb von 36 Monaten nach Veröffentlichung im EU-Amtsblatt, alle Anforderungen zu erfüllen. Viele Automatisierungsprodukte fallen unter diese Regulierung. Bislang richtete sich alle Cybersecurity-Regulierung an Betreiber: sie sind Risikoeigentümer, sie müssen Risikoanalysen machen, Vorfälle melden und die Resilienz ihrer Anlagen gegen Cyber-Angriffe nachweisen. Jetzt besteht eine Riesenchance für Betreiber, den Dialog über Cybersecurity-Anforderungen mit ihren Herstellern auf eine neue, konstruktivere Ebene zu heben.

Gerade bei Automatisierungssystemen sind Betreiber aber abhängig davon, dass Hersteller ihnen sichere Komponenten liefern: mit Security-Features, ohne Schwachstellen, und mit ausreichender Dokumentation, damit Betreiber das mit den Komponenten verbundene Cybersecurity-Risiko überhaupt abschätzen können. Schon dieser letzte Punkt ist oft ein Problem: Ohne die Information, welche Kommunikationsprotokolle und Softwarebibliotheken in einer Komponente verwendet werden, hat ein Betreiber aus Security-Sicht ein Kuckucksei in seiner Anlage – eine fremde Komponente, für deren Security er plötzlich trotzdem verantwortlich ist.

Ein CE-Kennzeichen für Security

Der Cyber Resilience Act (CRA) ist eine EU-Verordnung, die bestimmte Cybersecurity-Anforderungen für alle „products with digital elements“ verpflichtend macht – die weltweit erste Verordnung dieser Art für Produkthersteller. Sie hat bereits den Konsens der EU-Kommission, des europäischen Rates und des europäischen Parlaments gefunden und wird voraussichtlich Ende 2024 in Kraft treten. Ab 2027 muss damit jedes digitale Produkt, das auf dem europäischen Binnenmarkt in Verkehr gebracht wird, den CRA erfüllen. Betroffene Produkte sind alle, die eine Verbindung zu anderen aufbauen können und digitale Darten verarbeiten. Das ist ein sehr großer Anwendungsbereich.

Der CRA erweitert das bewährte CE-Kennzeichen um Cybersecurity. Das CE-Kennzeichen bringen Hersteller auf betroffenen Produkten an, um auszuweisen, dass sie die Sicherheitsbestimmungen für das Produkt relevanten EU-Regulierungen erfüllen. Das gibt es beispielsweise für Sonnenbrillen (die einen bestimmen UV-Schutz sicherstellen müssen), Druckbehälter (die vor Bersten geschützt sein müssen) und Kinderspielzeug (das die Gesundheit der Kinder nicht gefährden darf) – und nun eben auch für digitale Produkte, die nicht als Einfallstore für Cyber-Angriffe dienen dürfen.

Harmonisierte Standards lassen noch auf sich warten

Wie bei anderen Verordnungen rund um das CE-Kennzeichen soll es harmonisierte europäische Normen (hEN) geben, die die eher vage beschrieben Cybersecurity-Anforderungen aus dem CRA konkretisieren. Solche Normen anzupassen bzw. neu zu schreiben, ist für den riesigen Anwendungsbereich des CRA aber eine Mammutaufgabe. Die hEN wird es deswegen erst Monate bis Jahre nach Inkrafttreten des CRA geben, und auch erst einmal nur für „important“ und „critical products“, die in den Anhängen des CRA gelistet werden.

Die meisten Automatisierungskomponenten gehören nicht dazu – auch wenn es kein Geheimnis ist, dass die Standards der IEC-62443-Normenreihe heiße Kandidaten für hENs im Automatisierungsbereich sind. Auch ohne hENs muss der CRA aber bis 2027 erfüllt werden – was bedeutet, dass Hersteller von Automatisierungskomponenten vorerst ihren eigenen Weg finden müssen, die Anforderungen des CRA im Detail zu interpretieren und umzusetzen.

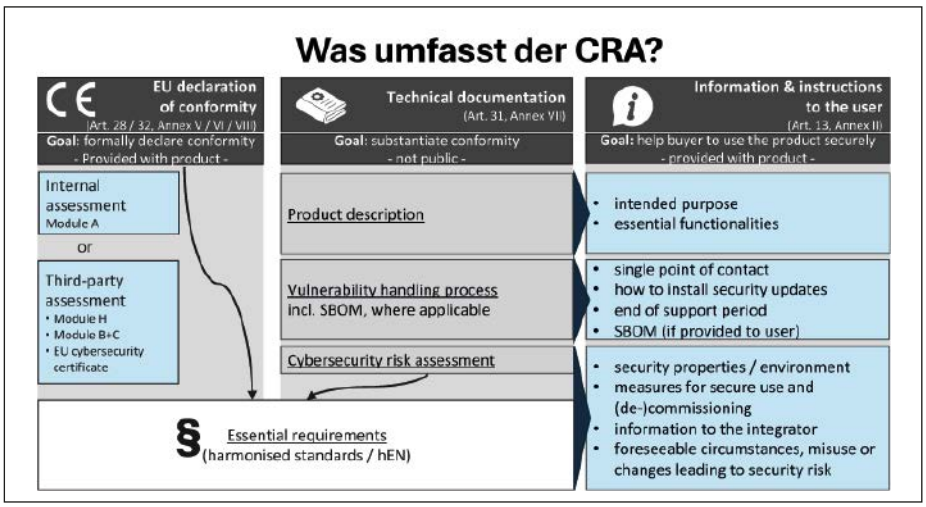


Abb. 1: Was der Cyber Resilience Act fordert.

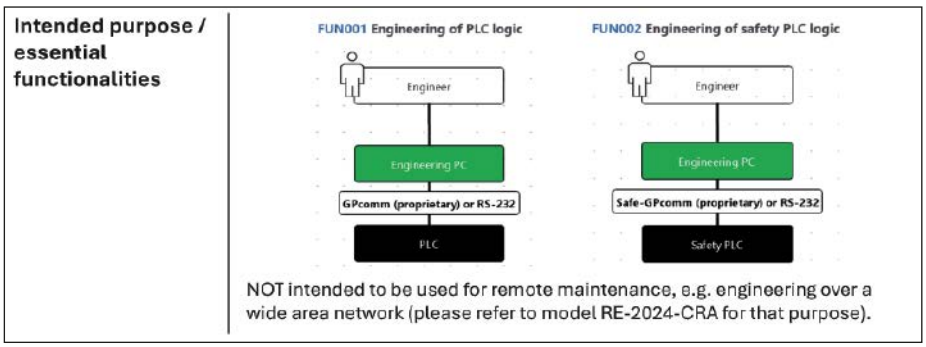
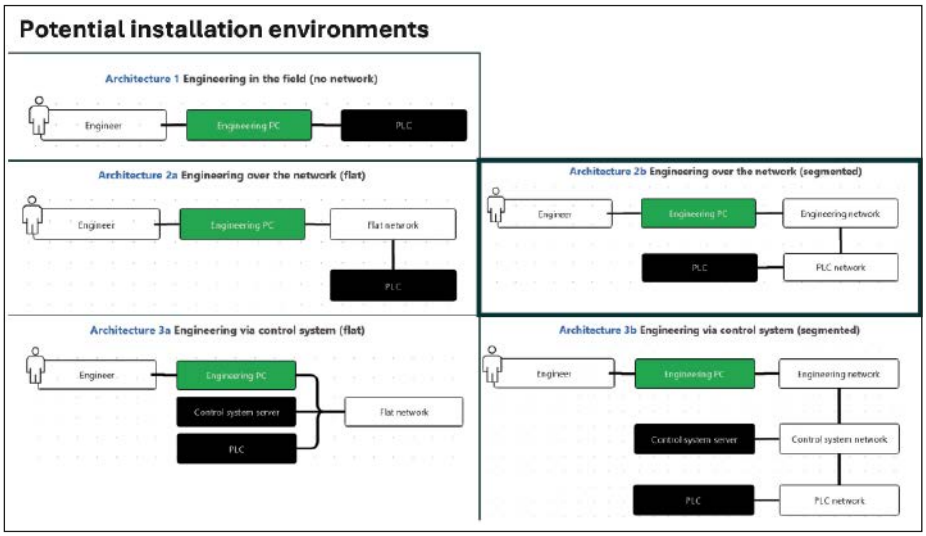


Abb. 2: Darstellung der Verwendungszwecke für einen Engineering-PC (grün)



Bilder © Admerita

Abb. 3: Mögliche Einbauumgebungen für den Engineering-PC (grün)

Das Problem mit den Security-Anforderungen an Hersteller

Wenn es um das Festlegen von Cybersecurity-Anforderungen für Produkte geht, tun sich Hersteller von Automatisierungskomponenten und Anlagenbetreiber oft schwer:

Betreiber wissen nicht genau, was sie fordern sollen und legen Herstellern in Ermangelung von Alternativen oft entweder sehr

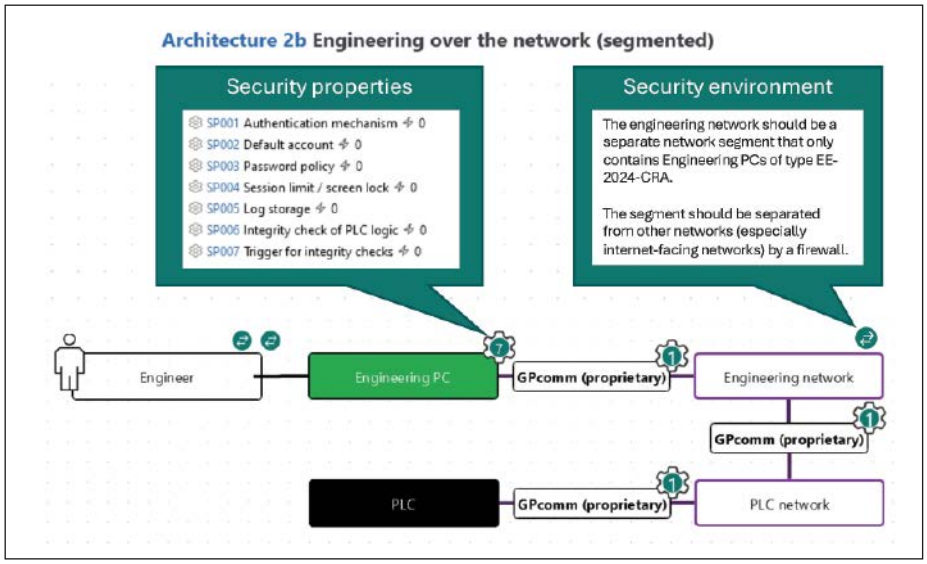


Abb. 4: Security-Eigenschaften (blaugrüne Icons) für den Engineering-PC (grün) und seine Umgebung am Beispiel der Einbauumgebung 2b

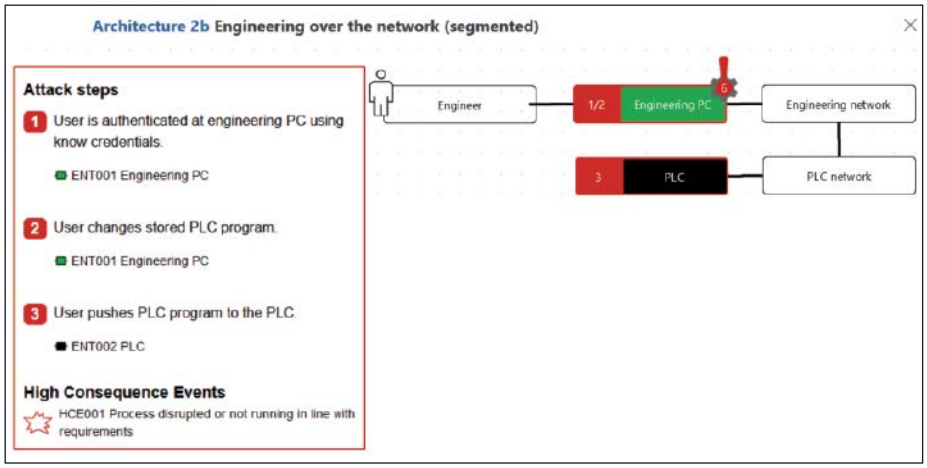


Abb. 5: Beispielhaftes Risikoszenario für den Engineering-PC (grün)

generische Forderungen („Security muss berücksichtigt werden!“) oder aber lange Listen von Security-Anforderungen vor, die auf dem Markt niemand vollumfänglich erfüllen kann. Wenn Hersteller über Cybersecurity sprechen, schwingt aufseiten der Betreiber oft ein gewisser Argwohn mit: „Die wollen uns doch nur neue Hard- und Software verkaufen!“.

Hersteller wiederum sind frustriert von unerfüllbaren Anforderungen und betreiberseitig fehlender Begeisterung für die Security-Eigenschaften, die ihre Produkte bereits haben: „Wir haben eine normale und eine „secure“-Variante unseres Produktes – raten Sie mal, was die Kunden kaufen. Wir würden ja gern alle Security der Welt in unsere Produkte einbauen…. Wenn denn jemand bereit wäre, dafür zu zahlen.“

Der CRA wird bei der Definition von Security-Anforderungen helfen – langfristig zumindest. Wie bei anderen Verordnungen rund um das CE-Kennzeichen soll es harmonisierte europäische Normen (hEN) geben, die Cybersecurity-Anforderungen aus dem CRA konkretisieren.

Solche Normen anzupassen bzw. neu zu schreiben, ist für den riesigen Anwendungsbereich des CRA aber eine Mammutaufgabe. Die hEN wird es deswegen erst Monate bis Jahre nach Inkrafttreten des CRA geben, und auch erst einmal nur für „important“ und „critical products“, die in den Anhängen des CRA gelistet werden. Die meisten Automatisierungskomponenten gehören nicht dazu – auch wenn es kein Geheimnis ist, dass die Standards der IEC-62443-Normenreihe heiße Kandidaten für hENs im Automatisierungsbereich sind.

Auch ohne hENs müssen die „essential requirements“ des CRA aber bis 2027 erfüllt werden. Und selbst ohne hENs birgt er schon eine große Chance für Betreiber, in ihren Forderungen an Hersteller konkreter zu werden.

Drei Dokumente für die CRA-Compliance

Was Hersteller tun müssen, damit sie das CE-Kennzeichen auf ihren Produkten anbringen dürfen, fasst Abb. 1 zusammen.

Die „anfassbaren“ Ergebnisse sind im Wesentlichen drei Dokumente, die Hersteller erstellen müssen:

- 1. Die Konformitätserklärung (EU declaration of conformity) ist ein kurzes Dokument, das die Konformität mit den „essential requirements“ des CRA bzw. den relevanten hENs erklärt. Sie wird mit dem Produkt mitgeliefert bzw. öffentlich verfügbar gemacht.
- 2. Die technische Dokumentation (technical documentation) ist die umfassende Dokumentation, die als Beleg der Konformität dient. Sie ist nicht öffentlich, wird aber der Instanz vorgelegt, die die Prüfung durchführt, und die Marktaufsichtsbehörden (in Deutschland wahrscheinlich das BSI) können jederzeit Einsicht fordern. Die Herausforderung liegt hier nicht zuvordertst in der Dokumentation, sondern darin, die zugrundeliegenden Prozesse, die der CRA in seinen „essential requirements“ vom Hersteller fordert – Integration von Security in die Produktentwicklung, Schwachstellenmanagement und Risikoamanagement – tatsächlich zu leben.
- 3. Die Informationen und Anleitungen für den Nutzer (information & instructions to the user) kann man als Auszug daus der technischen Dokumentation verstehen. Sie wird dem Produkt bei Kauf beigelegt und enthält alle Informationen, die für den Käufer des Produktes wichtig sind.

Vor allem das Dokument zu Punkt 3, die Nutzeranleitung, wird unterschätzt. Wahrscheinlich, weil wir dabei Benutzerhandbücher für Verbraucher im Kopf haben, die jedem Produkt beiliegen – und die sowieso nie jemand liest. Und dasselbe Schicksal wird wahrscheinlich die CRA-Benutzerhandbücher ereilen, die Verbraucherprodukten beiliegen. Wer hat schon Zeit, sich mit den Security-Eigenschaften seiner neuen Funkmaus zu befassen?

Aber Käufer von Automatisierungskomponenten sind keine normalen Verbraucher. Sie stecken die Produkte nicht einfach nur in die Steckdose, sondern sie integrieren sie – oft mit beachtlichen eigenen Engineering-Aufwänden – in komplexe Anlagen. Und für die Cybersecurity dieser Anlagen sind sie verantwortlich; sie sind Risikoeigentümer und oft selbst reguliert.

Chancen für Betreiber

Für diese Käufer, die Anlagenbetreiber, ist diese unscheinbare Benutzeranleitung eine riesige Chance: Eine Chance, endlich in strukturierter Form die Informationen zu erhalten und fordern

zu können, die sie für ihre Risikoeinschätzungen brauchen. Eine Chance, vom Hersteller mehr als eine lange Liste von Security-Eigenschaften vorgelegt zu bekommen, die sie als Betreiber nicht einschätzen können. Eine Chance, selbst zu entscheiden, welche Rolle eine neue Komponente in ihrem Security-Konzept spielt – und entsprechende Forderungen präzise zu stellen.

Und für Hersteller kann eine ernstgenommene Nutzeranleitung einen missmutigen Betreiber, der die Security-Features der Komponenten nicht versteht und dafür nicht bezahlen möchte zu einem zufriedenen Kunden machen.

Eine gute Nutzeranleitung fordern

Was würde Betreibern helfen? Vier leicht umsetzbare Anregungen für gute Nutzeranleitungen:

- 1. Verwendungszwecke mit Diagrammen verdeutlichen, die für jeden Verwendungszweck das Zusammenspiel von technischen Komponenten, Kommunikationsprotokollen und (ggf.) Menschen darstellen (Abb. 2).
- 2. Mögliche Einbauumgebungen zur Auswahl stellen: Ein Grund, warum Hersteller keine konkreten Hilfestellungen für Security-Eigenschaften von Komponenten geben? Das hängt von der Einbauumgebung ab – und die kennen sie ja schließlich nicht. Das Problem ist lösbar: Beispielsweise, indem man verschiedene typische Einbauumgebungen zur Auswahl stellt und Empfehlungen in Abhängigkeit der ausgewählten Architektur gibt (Beispiel in Abb. 3).
- 3. Security-relevante Eigenschaften explizit kennzeichnen: Für eine ausgewählte Einbauumgebung fällt es dann auch viel leichter, explizit die security-relevanten Eigenschaften der Komponente hervorzuheben – idealerweise mit Empfehlungen, wie diese Eigenschaften konfiguriert werden sollten. Auch Empfehlungen für Komponenten in der Umgebung können so transportiert werden (Beispiel in Abb. 4).
- 4. Berücksichtigte Risikoszenarien mitliefern: Wenn der Betreiber selbst Risikoanalysen machen muss, hilft es ihm enorm, wenn er die berücksichtigten Bedrohungsszenarien für die verwendeten Komponenten kennt. So kann er verstehen, woher die Empfehlungen für Security-Eigenschaften rühren – und im Idealfall kann er die Szenarien direkt in seine eigene Risikoanalyse übernehmen (Beispiel in Abb. 5).

Noch ist der CRA für alle neu. Alle Hersteller finden gerade ihren Weg, damit umzugehen. Keiner hat eine genaue Vorstellung, wie die „information & instructions to the user“, diese wichtige Schnittstelle zwischen Hersteller und Betreiber, aussehen wird.

Wenn Betreiber wollen, dass es ein Dokument wird, das ihnen wirklich hilft, statt eines, dass sie seufzend und ungelesen abheften, ist jetzt der richtige Zeitpunkt, Pflöcke einzuschlagen und Forderungen zu machen. Und für Hersteller? Für sie ist es die Chance, als leuchtendes Beispiel zu glänzen: Endlich mal jemand, der die Security-Wünsche seiner Kunden kennt und erfüllt.

Referenz

[1] Die aktuellste öffentlich verfügbare Fassung des CRA ist die am 10.10.2024 vom Europäischen Rat verabschiedete Version: https://data.consilium.europa.eu/doc/document/PE-100-2023-INIT/en/pdf

Dr. Sarah Fluchs,
CTO, Admeritia

Wiley Online Library

admeritia GmbH, Langenfeld
sarah.fluchs@admeritia.de
www.admeritia.de