idw - Informationsdienst Wissenschaft
Nachrichten, Termine, Experten

Pressemitteilung

Fraunhofer-Institut für Entwurfstechnik Mechatronik
Kirsten Harting-Stuke

11.10.2024
http://idw-online.de/de/news841094

Forschungs- / Wissenstransfer, Organisatorisches
Elektrotechnik, Informationstechnik, Maschinenbau, Wirtschaft
überregional

Cyber Resilience Act der EU verabschiedet: Drei Sofortmaßnahmen für Unternehmen

Lange wurde der Cyber Resilience Act (CRA) angekündigt, nun ist es offiziell: Am 10. Oktober 2024 ist er verabschiedet worden. Damit gelten ab dem November 2027 für eine Vielzahl vernetzter Geräte und deren Software EU-weite neue Mindestanforderungen in puncto Security – Schwachstellenmeldepflichten gelten sogar schon ab August 2026. Vor allem die Hersteller von Produkten werden in die Pflicht genommen: Sie müssen sicherstellen, dass ihre Produkte die Sicherheitskriterien für den europäischen Markt erfüllen, und zwar mit wenigen Ausnahmen, unabhängig der Branche.

Das Fraunhofer IEM erarbeitet mit Unternehmen wie adesso mobile solutions, Connext, Phoenix Contact und Kraft Maschinenbau seit vielen Jahren Security-Maßnahmen – und gibt Tipps, wie Unternehmen sich für den CRA rüsten können. „Die Übergangsfrist, bis der CRA 2027 voll erfüllt werden muss ist kurz. Unternehmen müssen sich in vielen Bereichen neu aufstellen – angefangen von der Durchführung von Security-Risikoanalysen über kurzfristige Meldepflichten bei Bekanntwerden von Schwachstellen bis hin zu kostenfreien Security-Updates während der erwarteten Lebensdauer des Produkts. Und Aufschieben gilt nicht, denn bei Nichteinhaltung des CRA drohen Strafzahlungen in Millionenhöhe“, erläutert Dr. Matthias Meyer, Bereichsleiter Softwaretechnik und IT-Sicherheit am Fraunhofer IEM.

Das Forschungsinstitut empfiehlt Unternehmen jetzt drei Maßnahmen zu ergreifen, um den Weg zur CRA-konformen Produktentwicklung zu beginnen. „Die schnelle Reaktion auf das Bekanntwerden von Schwachstellen und systematische Risikoanalysen sind essenzielle Maßnahmen zur Erfüllung der CRA-Anforderungen: Unternehmen, die diese Maßnahmen jetzt angehen, sind schon sehr gut unterwegs. Zusätzlich bringt eine Ist-Stands-Analyse im Hinblick auf die Produkte und Prozesse Klarheit für das weitere Vorgehen“, betont Dr. Meyer.

Erstens: Aufbau eines Schnelleinsatzteams für den Ernstfall

Werden Hersteller gewahr, dass Schwachstellen in ihren Produkten ausgenutzt werden, müssen sie künftig die Agentur der Europäischen Union für Cybersicherheit (ENISA) umgehend informieren: Innerhalb von 24 Stunden müssen sie eine erste Warnung geben und innerhalb von 72 Stunden weitere Details zur Art der Schwachstelle, möglichen Gegenmaßnahmen und mehr liefern. Abgesehen davon müssen sie jederzeit ansprechbar sein für Personen, die Sicherheitslücken melden möchten, und im Blick behalten, ob Schwachstellen in einem zugelieferten Softwarebestandteil bekannt werden. Dies gehört zu den Aufgaben eines Product Security Incident Response Teams (PSIRT): Hersteller, die noch kein PSIRT etabliert haben, sollten sich dringend damit befassen, denn die genannten Pflichten sind bereits ab Juni 2026 zu erfüllen, und zwar für alle Produkte auf dem Markt, auch solche, die lange vor Inkrafttreten des CRA lanciert wurden.

Zweitens: Bedrohungs- und Risikoanalysen als zentrales Instrument

Im Kern verlangt der CRA, dass Hersteller ihre Produkte regelmäßig auf Sicherheitsrisiken analysieren und an diese Risiken angepasste Sicherheitsmaßnahmen integrieren. Unternehmen müssen das Durchführen von Bedrohungs- und Risikoanalysen für alle Produkte fest in den Entwicklungsprozess integrieren: So identifizieren sie systematisch Bedrohungen, bewerten das jeweilige Sicherheitsrisiko und leiten informiert und gezielt Schutz- und Gegenmaßnahmen ab. Das Sicherheitsniveau der Software kann somit kontinuierlich und vor allem angemessen erhöht werden. Entwickler:innen erlangen ein neues Sicherheitsbewusstsein und teure, aber eigentlich unnötige Maßnahmen werden sogar vermieden.

Drittens: Überblick durch Ist-Stand-Analyse

Die ersten beiden Maßnahmen sind wichtig, werden aber nicht ausreichen: Unternehmen müssen sich ein Bild davon machen, welche Anforderungen des CRA sie erfüllen, und zwar sowohl bezüglich ihrer Prozesse im Produktlebenszyklus als auch der konkreten Produkte. Auch wenn noch keine harmonisierten Normen zum CRA vorliegen, ist einhellige Expertenmeinung, dass der bereits existierende Standard für industrielle Cybersicherheit IEC 62443 eine sehr gute Orientierung gibt. Unternehmen müssen also nicht warten, sondern können schon jetzt Ist-Stands-Analysen für ihre Prozesse und Produkte durchführen und Maßnahmen ableiten und somit wertvolle Zeit bei der Umsetzung des CRA gewinnen.

Zusammenarbeit mit Phoenix Contact, Miele und weiteren Unternehmen

Die Expertise des Fraunhofer IEM stützt sich auf langjährige Projekterfahrungen mit Unternehmen. So unterstützten die Wissenschaftler:innen bereits 2018 Phoenix Contact dabei, sich als eines der ersten Unternehmen nach der Cybersicherheitsnorm IEC 62443-4-1 zertifizieren zu lassen, indem sie eine auf Phoenix Contact angepasste Methode zur Bedrohungs- und Risikoanalyse erarbeiteten.

Seitdem hat das Fraunhofer IEM die Methode stetig weiterentwickelt und in zahlreichen Bedrohungsanalyse-Workshops und Schulungen angewendet, z. B. mit Kraft Maschinenbau. „Wir profitieren nicht nur von einer Risikobewertung für unsere Produkte. Unsere Mitarbeiter:innen erlernten im Workshop mit dem Fraunhofer IEM auch ein systematisches Vorgehen für künftige Bedrohungsanalysen und steigerten ihr Sicherheitsbewusstsein", sagt Geschäftsführer Jörg Timmermann.

Um sicherzustellen, dass seine langlebigen Produkte auch nach Markteinführung sicher bleiben, stellte Miele mit dem Fraunhofer IEM bereits im Jahr 2021 ein eigenes PSIRT-Team auf. Durch Stakeholder-Interviews gelang es, auf bestehenden Unternehmensprozessen aufzubauen und klar definierte Prozess-Schnittstellen zu schaffen.

In Vorbereitung auf die Norm für industrielle Cybersicherheit IEC 62443 ermittelte KEB den Ist-Stand seiner Entwicklungsprozesse. Das Fraunhofer IEM führte dazu Interviews mit Führungskräften und Safety-Expert:innen des Unternehmens durch und half KEB, weitere nötige Tätigkeiten zur Umsetzung der Norm zu planen, deren Aufwand abzuschätzen und die Normumsetzung systematisch voranzutreiben.

Damit alle an der Softwareentwicklung beteiligten Mitarbeitenden auf dem Laufenden bleiben und ihre Softwareentwicklung stets verbessern, arbeitet das Fraunhofer IEM auch im Bereich der Mitarbeitenden-Weiterbildung z.B. mit adesso mobile solutions und Connext zusammen. Beide Unternehmen setzen schon seit vielen Jahren Security Champions als Multiplikatoren für das Thema Cybersecurity in ihrer Softwareentwicklung ein.

wissenschaftliche Ansprechpartner:

Dr. Matthias Meyer (matthias.meyer@iem.fraunhofer.de)
Dr. Markus Fockel (markus.fockel@iem.fraunhofer.de

URL zur Pressemitteilung: https://www.youtube.com/watch?v=qWp_kLCl4oc

In seinem Secure Engineering Lab in Paderborn unterstützt das Fraunhofer IEM Unter-nehmen dabei, ihre Prozesse und Produkte den neuen EU-Richtlinien anzupassen.
Fraunhofer IEM
Fraunhofer IEM