

CRA-Meldepflichten gelten: secuvera, Nuki und AV-TEST beleuchten den Praxistest für Hersteller

Gäufelden, 22. September 2026 – Seit dem 11. September 2026 gelten die ersten Meldepflichten des europäischen Cyber Resilience Act (CRA). Was die neuen Vorgaben für Hersteller vernetzter Produkte in der Praxis bedeuten, diskutierten Fachleute von Nuki, secuvera und AV-TEST im Paneltalk „Cyber Resilience Act & IoT-Sicherheit“. Die vom Hersteller Nuki initiierte Gesprächsrunde fand im Rahmen eines Pressefrühstücks am 3. September in Berlin statt.

Auf dem Panel sprachen die Nuki-Mitgründer Martin Pansy, CEO, und Jürgen Pansy, Chief Innovation Officer, Luise Werner, Cybersecurity-Beraterin bei secuvera, sowie Eric Clausing, IoT-Lead bei AV-TEST. Dabei kamen drei Perspektiven zusammen, die für wirksame Produktsicherheit ineinandergreifen müssen: die Umsetzung beim Hersteller, die regulatorische Einordnung und die unabhängige technische Prüfung.

Meldefristen werden zum Praxistest

Hersteller von Produkten mit digitalen Elementen müssen aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle innerhalb enger Fristen melden. Grundsätzlich ist innerhalb von 24 Stunden eine Frühwarnung erforderlich. Innerhalb von 72 Stunden folgt eine weitergehende Meldung mit den zu diesem Zeitpunkt verfügbaren Informationen und einer ersten Bewertung.

Dafür müssen Hersteller kurzfristig feststellen können, welche Produkte, Versionen und Komponenten betroffen sind, wie schwerwiegend ein Vorfall ist und welche Maßnahmen notwendig sind. Der Paneltalk zeigte: Cybersicherheit ist ein kontinuierlicher Prozess. Er reicht von der Risikobewertung und Security by Design über die Steuerung von Drittkomponenten und Lieferketten bis zu technischen Tests, Sicherheitsupdates und der Dokumentation sicherheitsrelevanter Entscheidungen.

„Die neuen Meldepflichten sind vor allem ein Praxistest für die Sicherheitsorganisation der Hersteller. Innerhalb kürzester Zeit muss belastbar geklärt werden können, welche Produkte und Versionen betroffen sind, wie schwerwiegend ein Vorfall ist und welche Maßnahmen notwendig sind“, sagt Luise Werner. „Das funktioniert nur, wenn Risikoanalyse, sichere Entwicklung, technische Tests und Schwachstellenmanagement schon vorher ineinandergreifen.“

Security by Design trifft unabhängige Prüfung

Nuki brachte die Perspektive eines Herstellers vernetzter Produkte in die Gesprächsrunde ein. Das Unternehmen für smarte Zutrittslösungen setzt nach eigenen Angaben seit der ersten Smart-Lock-Generation auf Security by Design und berücksichtigt Sicherheitsanforderungen über den gesamten Produktlebenszyklus hinweg.

„IT-Sicherheit ist für uns kein nachträglicher Anstrich, den man einem Produkt verleiht, wenn eine neue Verordnung kommt – sie ist in unserer Produkt-DNA verankert“, sagt Jürgen Pansy, Mitgründer und Chief Innovation Officer von Nuki.

AV-TEST ergänzte die Diskussion um die Perspektive eines unabhängigen Prüfinstituts. Technische Sicherheitstests zeigen, ob vorgesehene Sicherheitsmaßnahmen auch in der konkreten Implementierung wirksam sind.

„Ein Produkt kann auf dem Papier sicher sein und trotzdem angreifbar. Unabhängige Sicherheitstests schaffen eine wichtige zusätzliche Perspektive“, sagt Eric Clausing, IoT-Lead bei AV-TEST.

Der Paneltalk verdeutlicht: Herstellerpraxis, Compliance und unabhängige Prüfungen müssen ineinandergreifen, damit vernetzte Produkte die regulatorischen Anforderungen erfüllen und ihre Sicherheitsmaßnahmen auch in der Praxis wirksam sind.

Über secuvera GmbH

secuvera ist ein unabhängiger IT-Sicherheitsdienstleister mit Schwerpunkt auf Prüf- und Beratungsleistungen in der Cybersicherheit. Als vom Bundesamt für Sicherheit in der Informationstechnik (BSI) anerkannte Prüfstelle führt secuvera Zertifizierungsprüfungen für IT-Produkte und digitale Anwendungen nach nationalen und internationalen Standards durch. Hierzu zählen unter anderem Prüfungen nach Common Criteria und IEC 62443 (Industrial Security), die im Rahmen der Anerkennung als IT-Sicherheits-Evaluierungsstelle (ITSEF) erfolgen.

Ergänzend unterstützt das Unternehmen mit Sitz in Gäufelden bei Stuttgart Organisationen in den Bereichen Informationssicherheitsmanagement (BSI-Grundschutz, ISO 27001, IS-Revision), Penetrationstests und Red-Teaming sowie bei der Einordnung und Umsetzung regulatorischer Anforderungen wie NIS-2 und dem Cyber Resilience Act (CRA).

Zum Kundenspektrum gehören Industrieunternehmen, Behörden, Betreiber kritischer Infrastrukturen und Organisationen mit hohen Sicherheitsanforderungen in der DACH-Region und weltweit.

Weitere Informationen zu secuvera finden Sie unter www.secuvera.de.

Herausgeber der Meldung:

secuvera GmbH

Siedlerstraße 22-24
DE 71126 Gäufelden
Tel.: +49 07032 97580
www.secuvera.de

Kontakt für Medienanfragen:

secuvera GmbH

Anna Schmidt
Marketing & Communications
Tel.: +49 7032 975897
E-Mail: aschmidt@secuvera.de