



PRESSEMITTEILUNG

CRA-Start: Nuki sieht Security-by-Design-Kurs bestätigt und fordert faire Wettbewerbsbedingungen

Graz, am 8. September 2026

Am 11. September 2026 läutet die EU mit den ersten Meldepflichten des Cyber Resilience Act (CRA) eine neue Ära für vernetzte Produkte ein: Cybersicherheit wird von der Ermessenssache zur gesetzlichen Pflicht. Bei Nuki sieht man diesem Stichtag gelassen entgegen: Security-by-Design ist beim Pionier für smarten Zutritt seit mehr als zehn Jahren gelebter Standard. Zugleich macht sich das österreichische Unternehmen für eine lückenlose Durchsetzung der neuen Spielregeln stark.

Der smarte Rauchmelder schickt bei Alarm sofort eine Push-Nachricht, die Kaffeemaschine startet per App, das elektronische Türschloss lässt die Reinigungskraft ins Haus. Wer digitalen Alltagshelfern vertraut, muss sich darauf verlassen können, dass die Privatsphäre und das Zuhause lückenlos geschützt sind. Bislang war IT-Sicherheit oft reine Ermessenssache der Hersteller. Der Cyber Resilience Act (CRA) der Europäischen Union schafft jetzt klare Regeln und macht Cybersicherheit zur verpflichtenden Anforderung über den gesamten Produktlebenszyklus hinweg: von der Entwicklung über den Verkauf bis zur langjährigen Software-Pflege. Die Regelung betrifft bei Weitem nicht nur IoT-Geräte: Sie gilt branchenübergreifend für praktisch alle Produkte mit digitalen Elementen – von reiner Software über IT-Infrastruktur bis zu vernetzter Hardware. Für bestimmte Produktgruppen gelten Ausnahmen: etwa in der Medizintechnik, der zivilen Luftfahrt oder bei bestimmten Fahrzeugtypen. Ab 11. Dezember 2027 müssen alle vernetzten Produkte, die in der EU in Verkehr gebracht werden, die Anforderungen des Cyber Resilience Act vollständig erfüllen.

Solides Fundament statt hektischer Ad-hoc-Maßnahmen

Für Nuki bestätigt die neue EU-Verordnung den seit der Firmengründung eingeschlagenen Kurs: konsequentes Security-by-Design. Dabei wird IT-Sicherheit nicht im Nachhinein aufgesetzt, sondern von der ersten Codezeile und Skizze an integriert. Ende-zu-Ende-Verschlüsselung, durchgängige Bedrohungsanalysen und nahtlose Sicherheitsupdates über das Internet sind bei Nuki seit der ersten Smart-Lock-Generation Standard. Auch hardwareseitig entwickelt Nuki seine Systeme kontinuierlich weiter – von physischen Secure Elements über erweiterten Speicherschutz bis hin zur Absicherung gegen Manipulationsversuche. *„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. Wir sehen den Cyber Resilience Act deshalb als konsequente Fortsetzung unseres bisherigen Kurses“,* betont Jürgen Pansy, Mitgründer und Chief Innovation Officer von Nuki. Zugleich ordnet er den Aufwand realistisch ein: *„Niemand schüttelt die Erfüllung der CRA-Anforderungen einfach aus dem Ärmel. Aber dank unserer Vorarbeit ist das für uns kein hektischer Umbau bei laufendem Betrieb, sondern strukturiertes Arbeiten auf einem sehr soliden Fundament.“*

24 Stunden, 72 Stunden: Der neue Takt der Cybersicherheit

Die erste CRA-Bewährungsprobe für Hersteller steht unmittelbar bevor: Am 11. September 2026 treten die Meldepflichten für aktiv ausgenutzte Schwachstellen und schwerwiegende Sicherheitsvorfälle in Kraft. Geht ein Hinweis auf einen Vorfall ein, tickt die Uhr. Hersteller müssen umgehend die technische Betroffenheit bewerten und Verantwortlichkeiten klären, um innerhalb von 24 Stunden eine offizielle Frühwarnung abzugeben. Binnen 72 Stunden folgt eine weitergehende Meldung mit den zu diesem Zeitpunkt verfügbaren Informationen und einer ersten Bewertung. IT-Sicherheit ist somit kein nachträgliches Dokumentationsprojekt und kein einmaliger Test am fertigen Produkt mehr, sie wird zu einem festen Bestandteil der Qualitätssicherung – von der ersten Risikoanalyse über die Entwicklung bis hin zur jahrelangen Produktpflege im Feld. *„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. Das funktioniert nur, wenn Risikoanalyse, sichere Entwicklung, technische Tests und Schwachstellenmanagement schon vorher ineinandergreifen“,* betont Luise Werner, Cybersecurity-Expertin bei secuvera, BSI-zertifizierter IT-Sicherheitsdienstleister und anerkannte Prüfstelle.

Der Praxistest macht den Unterschied

Dass saubere Prozesse auf dem Papier allein noch keinen Schutz garantieren, zeigt der Blick in die Prüfpraxis. *„Ein Produkt kann auf dem Papier sicher sein und trotzdem angreifbar. Unabhängige Sicherheitstests schaffen eine wichtige zusätzliche Perspektive“,* betont Eric Clausing, IoT-Lead bei AV-TEST. Ein Großteil der in der Praxis identifizierten Schwachstellen entstehe nicht durch Lücken im theoretischen Konzept, sondern durch Fehler bei der Implementierung. Technische Prüfungen – von der Online-Kommunikation über mobile Apps bis zur Hardware – seien essenziell, um formale Vorgaben und praktische Sicherheit zu verknüpfen. Dass der CRA einen verbindlichen Rahmen für vernetzte Produkte vorgibt, sieht Clausing rundum positiv: *„Für Hersteller bedeutet das nicht nur zusätzliche Anforderungen, sondern auch die Chance, Sicherheit messbar und nachvollziehbar zu machen. Unabhängige Prüfungen helfen, Vertrauen in die Sicherheit eines Produkts zu schaffen – bei Herstellern ebenso wie bei Nutzern.“*

Lücke zwischen technischer Realität und Wahrnehmung

Genau diese nachweisbare Sicherheit ist der Schlüssel, um ein zentrales Branchenproblem zu lösen. Obwohl etablierte Smart Locks ein hohes Sicherheitsniveau bieten, klafft zwischen technischer Realität und Wahrnehmung der Konsumentinnen und Konsumenten oft noch eine Lücke. Eine aktuelle Kundenbefragung von Nuki zeigt: Für 44 Prozent¹ zählen Sicherheitsbedenken zu den größten Hemmschwellen vor dem Erstkauf eines elektronischen Türschlosses. Das bestätigt auch eine kürzlich veröffentlichte Studie von Parks Associates im Auftrag der Connectivity Standards Alliance², die Datenschutz- und Sicherheitsbedenken ebenfalls als Hürde für die weitere Verbreitung von Smart-Home-Produkten identifiziert. *„Deshalb begrüßen wir den Cyber Resilience Act ausdrücklich. Gesetzliche Rahmenbedingungen wie der CRA, aber auch verlässliche Branchenstandards wie Matter und Siegel von unabhängigen Testinstituten wie AV-TEST helfen dabei, unbegründete Ängste abzubauen. Sie schaffen das Vertrauen, das wir brauchen, um Smart Locks für die breite Bevölkerung relevant zu machen“,* erklärt Martin Pansy, Mitgründer und CEO von Nuki.

Wenn Compliance zur Wettbewerbsfrage wird

So positiv Nuki die neuen gesetzlichen Rahmenbedingungen bewertet, so deutlich weist das Unternehmen auf die wirtschaftlichen Implikationen hin. Die EU-Kommission schätzt die direkten Compliance-Kosten auf rund 29 Milliarden Euro³ – rund zwei Prozent des europäischen Branchenumsatzes. Das ist laut Martin Pansy aber nur die halbe Wahrheit: *„Die Pflicht, ein Produkt fünf Jahre und länger mit Sicherheitsupdates zu versorgen, bindet dauerhaft Entwickler-Ressourcen. Dazu kommen Mehrausgaben bei Teileauswahl und Software-Tools.“* Eine Belastung, die für ein etabliertes Unternehmen wie Nuki stemmbar ist, für junge Start-ups jedoch eine erhebliche Markteintrittshürde darstellt und die europäische Innovationskraft hemmen kann. Vor diesem Hintergrund fordert Martin Pansy eine strikte Marktüberwachung: *„Der CRA setzt die richtigen Maßstäbe – doch eine EU-Verordnung ist nur so stark wie ihre Durchsetzung. Strenge Auflagen nützen Verbraucherinnen und Verbrauchern wenig, wenn Produkte ohne nachgewiesene Sicherheitsstandards weiterhin ungehindert auf den europäischen Markt gelangen. Wir brauchen chancengleiche Wettbewerbsbedingungen, die Verantwortung belohnen und nicht das Umgehen von Verordnungen.“*

Begleitendes Bildmaterial zu dieser Pressemitteilung steht unter diesem [LINK](#) bereit.
Weiterführende Informationen zu Nuki sowie allgemeines Bildmaterial finden Sie im [Pressebereich](#).

¹ Nuki Brand Survey 2025: Befragung vom 30. April 2025 unter 1305 Nuki-Club-Mitgliedern, die in den 6 Monaten vor der Umfrage ein Smart Lock von Nuki gekauft haben.

² Parks Associates: Whitepaper „Smart Home Evolution: Unlocking Value“ (erstellt für die Connectivity Standards Alliance), 2025.
Abrufbar unter diesem [Link](#).

³ Europäische Kommission: Commission Staff Working Document SWD(2022) 282 final, Abschnitt 6.3.1, 15.09.2022. Abrufbar unter diesem [Link](#).

Über Nuki Home Solutions

Die erfolgreiche Crowdfunding-Kampagne auf der Plattform Kickstarter legte 2015 den Grundstein für die Nuki-Erfolgsgeschichte. Seit damals wuchs das von den Brüdern Martin Pansy (CEO) und Jürgen Pansy (Chief Innovation Officer) in Graz gegründete Unternehmen stetig: Heute ist Nuki Europas führender Anbieter für smarte, nachrüstbare Zutrittslösungen. Nuki beschäftigt am Firmensitz in Graz aktuell mehr als 130 Mitarbeitende aus 18 verschiedenen Nationen. Das österreichische Unternehmen ist doppelt ISO-zertifiziert: ISO 9001 und ISO 14001 bescheinigen hohe internationale Standards in Sachen Qualitäts- und Umweltmanagementsystem. Neben dem in Europa produzierten Smart Lock sowie einem umfangreichen Zubehör- und Serviceangebot arbeitet Nuki mit Nachdruck an der Weiterentwicklung smarter Zutrittslösungen für eine komplett schlüssellose Zukunft.

Pressekontakt
Weidhase Communications:
Florian Weidhase
nuki@weidhase.de

Pressekontakt
Nuki Home Solutions:
Martina Stix
martina.stix@nuki.io