PRESS RELEASE

Ahead of the CRA: Nuki Proves Its Security-by-Design Advantage and Urges Fair Competition

Graz (Austria), September 8, 2026

On September 11, 2026, the EU will usher in a new era for connected products as the first reporting obligations under the Cyber Resilience Act (CRA) take effect, turning cybersecurity from a matter of discretion into a legal requirement. Nuki approaches this deadline with confidence: Security-by-Design has been an established practice for the smart access pioneer for over a decade. At the same time, the Austrian company is advocating for the rigorous enforcement of these new rules across the industry.

The smart smoke detector sends an instant push notification when an alarm is triggered, the coffee machine starts via an app, and the electronic door lock lets the cleaner inside. Anyone who relies on these everyday digital helpers must be able to trust that their privacy and their home remain fully protected. Until now, IT security has often been left entirely to the discretion of the manufacturers. The European Union's Cyber Resilience Act (CRA) now establishes clear rules, making cybersecurity a mandatory requirement throughout the entire product lifecycle: from development and sales to long-term software maintenance. This regulation affects far more than just IoT devices: it applies across industries to virtually any product with digital elements – from standalone software and IT infrastructure to connected hardware. Exceptions apply to specific product categories, such as medical devices, civil aviation, and certain types of vehicles. Starting December 11, 2027, all connected products placed on the EU market must fully comply with the requirements of the Cyber Resilience Act.

A Solid Foundation Over Hectic Ad-Hoc Measures

For Nuki, the new EU regulation validates the course set since the company's founding: rigorous Security-by-Design. Rather than being treated as an afterthought, IT security is integrated from the very first line of code and initial sketch. End-to-end encryption, continuous threat analysis, and seamless over-the-air security updates have been standard at Nuki since the first Smart Lock generation. On the hardware side, Nuki also continuously evolves its systems – ranging from physical Secure Elements and enhanced memory protection to safeguards against tampering attempts.

"For us, IT security is not a coat of paint added to a product when a new regulation comes along – it is embedded in our product DNA. We therefore see the Cyber Resilience Act as a logical continuation of our path," emphasizes Jürgen Pansy, Co-founder and Chief Innovation Officer of Nuki. *At the same time, he offers a realistic assessment of the effort involved: "Nobody fulfills CRA requirements overnight. But thanks to our groundwork, for us this isn't a hectic overhaul during ongoing operations, but structured work built on a very solid foundation."*

24 Hours, 72 Hours: The New Pace of Cybersecurity
The first major CRA test for manufacturers is right around the corner: on September 11, 2026, reporting obligations for actively exploited vulnerabilities and severe security incidents take effect. Once a report of an incident comes in, the clock starts ticking. Manufacturers must immediately evaluate the technical impact and clarify responsibilities to submit an official early warning within 24 hours. Within 72 hours, a more detailed notification must follow, containing the information available at that time along with an initial assessment. IT security is thus no longer a downstream documentation exercise or a one-time test on the finished product; it becomes an integral component of quality assurance – from the initial risk analysis through development to years of product maintenance in the field.

"The new reporting obligations are, above all, a real-world test for a manufacturer's security setup. Within a very short window, companies must be able to reliably clarify which products and versions are affected, how severe an incident is, and what actions are necessary. This only works if risk analysis, secure development, technical testing, and vulnerability management are already seamlessly aligned," emphasizes Luise Werner, cybersecurity expert at secuvera, a BSI-certified IT security service provider and recognized testing body.

Real-World Testing Makes the Difference
A look into testing practice shows that clean processes on paper alone do not guarantee protection. *"A product can be secure on paper and still be vulnerable. Independent security testing provides a vital additional perspective," underscores* Eric Clausing, IoT Lead at AV-TEST. The vast majority of vulnerabilities identified in real-world scenarios stem not from flaws in the theoretical concept, but from implementation errors. Technical evaluations – covering everything from online communication and mobile apps to hardware – are essential to bridge formal specifications with practical security.

Clausing views the CRA's binding framework for connected devices as a thoroughly positive development: *"For manufacturers, this brings not just additional requirements, but also the opportunity to make security measurable and transparent. Independent testing helps build trust in a product's security – for manufacturers and end users alike."*

The Gap Between Technical Reality and Perception
Verifiable security is precisely the key to solving a central industry challenge. Although established smart locks offer a high level of security, a gap often remains between technical reality and consumer perception. A recent customer survey by Nuki shows that 44 percent[1] consider security concerns to be among the biggest hurdles before buying an electronic door lock for the first time. This is further corroborated by a newly released study by Parks Associates on behalf of the Connectivity Standards Alliance[2], which similarly identifies data privacy and security concerns as a barrier to the broader adoption of smart home devices. *"That is why we explicitly welcome the Cyber Resilience Act. Regulatory frameworks like the CRA, alongside reliable industry standards like Matter and seals from independent testing institutes such as AV-TEST, help dismantle unfounded fears. They build the trust we need to make smart locks relevant to the general public,"* explains Martin Pansy, Co-founder and CEO of Nuki.

When Compliance Becomes a Competitive Issue
As positively as Nuki views the new regulatory framework, the company points out the economic implications just as clearly. The European Commission estimates direct compliance costs at around 29 billion euros[3] – roughly two percent of European industry revenue. However, according to Martin Pansy, that is only half the story: *"The obligation to supply a product with security updates for five years or longer permanently ties up developer resources. On top of that come additional expenses for component selection and software tools."*

This is a burden that an established company like Nuki can manage, but for young startups, it represents a significant barrier to entry and could dampen European innovation. Against this backdrop, Martin Pansy calls for strict market surveillance: *"The CRA sets the right benchmarks – yet an EU regulation is only as strong as its enforcement. Strict requirements offer little benefit to consumers if products without proven security standards continue to enter the European market unchecked. We need a level playing field that rewards responsibility rather than circumvention of regulations."*

High-resolution press imagery matching this press release is available for download at this link.
For further information about Nuki as well as general media assets, please visit our Press Area.

[1] Nuki Brand Survey 2025: Survey conducted on April 30, 2025, among 1,305 Nuki Club members who purchased a Nuki Smart Lock in the 6 months prior to the survey.
[2] Parks Associates: Whitepaper "Smart Home Evolution: Unlocking Value" (prepared for the Connectivity Standards Alliance), 2025. Available at this link.
[3] European Commission: Commission Staff Working Document SWD(2022) 282 final, Section 6.3.1, September 15, 2022. Available at this link.

About Nuki Home Solutions
In 2015, the successful crowdfunding campaign on the Kickstarter platform laid the foundation for Nuki's success story. Since then, the company – founded by brothers Martin Pansy (CEO) and Jürgen Pansy (Chief Innovation Officer) in Graz – has grown steadily: Today, Nuki is Europe's leading provider of smart, retrofit access solutions. The company currently employs 130 people from 18 different nationalities at its headquarters in Graz. Nuki holds dual ISO certifications – ISO 9001 and ISO 14001 – attesting to its high international standards in quality and environmental management systems. In addition to its Europe-produced Smart Lock and a wide range of accessories and services, the Austrian company is committed to continuously developing smart access solutions for a completely keyless future.

For editorial inquiries and review units,
please reach out to:
Martina Stix
martina.stix@nuki.io
Münzgrabenstraße 92/4
8010 Graz, Austria