COMMUNIQUÉ DE PRESSE

Cyber Resilience Act : conforté dans son approche « Security-by-Design », Nuki appelle à des conditions de concurrence équitables

Graz (Autriche), le 8 septembre 2026

Le 11 septembre 2026, l'Union européenne entrera dans une nouvelle ère pour les produits connectés avec l'entrée en vigueur des premières obligations de signalement prévues par le Cyber Resilience Act (CRA), faisant de la cybersécurité non plus une question de choix, mais une obligation légale. Nuki aborde cette échéance avec confiance car depuis plus de dix ans, le pionnier de l'accès intelligent applique une approche « Security-by-Design ». Dans le même temps, l'entreprise autrichienne appelle à une application rigoureuse de ces nouvelles règles à l'ensemble du secteur.

Le détecteur de fumée connecté envoie instantanément une notification push lorsqu'une alarme se déclenche, la machine à café démarre via une application et la serrure électronique permet au personnel de ménage d'entrer. Tous ceux qui utilisent ces assistants numériques du quotidien doivent pouvoir compter sur une protection fiable et transparente de leur vie privée et de leur domicile. Jusqu'à présent, la sécurité informatique a souvent été laissée à la discrétion des fabricants. Le Cyber Resilience Act (CRA) de l'Union européenne établit désormais des règles claires, faisant de la cybersécurité une exigence obligatoire tout au long du cycle de vie d'un produit, du développement et de la commercialisation jusqu'à la maintenance logicielle sur le long terme. Cette réglementation va bien au-delà des seuls appareils connectés, elle s'applique à pratiquement tous les secteurs et à presque tous les produits intégrant des éléments numériques, du logiciel en tant que tel aux infrastructures informatiques et à tous les équipements connectés. Seules font exception certaines catégories de produits, comme les dispositifs médicaux, l'aviation civile et certains types de véhicules. À compter du 11 décembre 2027, tous les produits connectés mis sur le marché de l'UE devront être pleinement conformes aux exigences du Cyber Resilience Act.

Un fondement solide plutôt que des mesures prises dans l'urgence
Pour Nuki, cette nouvelle réglementation européenne vient confirmer l'orientation adoptée dès la création de l'entreprise qui consiste à intégrer rigoureusement la sécurité dès la conception (« Security-by-Design »). Plutôt que de considérer la sécurité informatique comme une fonctionnalité ajoutée a posteriori, Nuki l'intègre dès la toute première ligne de code et dès les premières esquisses du produit. Le chiffrement de bout en bout, l'analyse continue des menaces et les mises à jour de sécurité transparentes par Internet font partie des standards appliqués par Nuki depuis la première génération de Smart Lock. Sur le plan matériel,

Nuki fait également évoluer continuellement ses systèmes, notamment grâce à des composants de sécurité physiques, à une protection renforcée de la mémoire et à des dispositifs destinés à prévenir les tentatives de manipulation.

« *Pour nous, la sécurité informatique n'est pas une couche de peinture ajoutée à un produit lorsqu'une nouvelle réglementation entre en vigueur, elle est inscrite dans l'ADN même de nos produits. Nous considérons donc le Cyber Resilience Act comme la poursuite logique de la voie que nous avons choisie* », souligne Jürgen Pansy, cofondateur et Chief Innovation Officer de Nuki.

Il porte toutefois un regard réaliste sur les efforts nécessaires : « *Personne ne peut se mettre en conformité avec les exigences du CRA du jour au lendemain. Mais grâce au travail que nous avons réalisé en amont, il ne s'agit pas pour nous d'une refonte précipitée en cours de production, mais d'un travail structuré reposant sur des bases très solides* ».

24 heures, 72 heures : le nouveau rythme de la cybersécurité
Dès le 11 septembre 2026, les fabricants devront faire face à la première mise à l'épreuve du CRA. Les obligations de signalement des vulnérabilités activement exploitées et des incidents de sécurité graves entreront en vigueur.

Dès qu'un incident est signalé, le compte à rebours commence. Les fabricants doivent immédiatement évaluer son impact technique et déterminer les responsabilités afin de transmettre une première alerte officielle dans un délai de 24 heures. Dans les 72 heures, une notification plus détaillée doit suivre, contenant les informations disponibles à ce stade ainsi qu'une première évaluation de la situation.

La sécurité informatique n'est donc plus un simple exercice de documentation réalisé en aval ou un test ponctuel effectué sur un produit fini. Elle devient une composante à part entière de l'assurance qualité, depuis l'analyse initiale des risques et le développement jusqu'à plusieurs années de maintenance du produit sur le terrain.

« *Les nouvelles obligations de signalement constituent avant tout un test concret de l'organisation mise en place par les fabricants en matière de sécurité. Dans un délai très court, les entreprises doivent être capables de déterminer de manière fiable quels produits et quelles versions sont concernés, quelle est la gravité d'un incident et quelles mesures doivent être prises. Cela n'est possible que si l'analyse des risques, le développement sécurisé, les tests techniques et la gestion des vulnérabilités sont déjà parfaitement coordonnés* », souligne Luise Werner, experte en cybersécurité chez Secuvera, un prestataire de services de sécurité informatique certifié par le BSI et un organisme de test reconnu.

Les tests en conditions réelles font la différence
L'expérience acquise dans le domaine des tests montre que des processus parfaitement définis sur le papier ne suffisent pas à garantir la protection d'un produit.

« *Un produit peut être sécurisé sur le papier et malgré tout présenter des vulnérabilités. Des tests de sécurité indépendants apportent un point de vue complémentaire essentiel* », souligne Eric Clausing, responsable IoT chez AV-TEST.

La grande majorité des vulnérabilités identifiées dans des scénarios réels ne proviennent pas de failles dans le concept théorique, mais d'erreurs de mise en œuvre. Les évaluations techniques, couvrant aussi bien les communications en ligne que les applications mobiles et les composants matériels, sont donc essentielles pour faire le lien entre les spécifications formelles et la sécurité réelle du produit.

Pour Eric Clausing, le cadre contraignant instauré par le CRA pour les appareils connectés constitue une évolution résolument positive : « *Pour les fabricants, cela implique non seulement des exigences supplémentaires, mais aussi la possibilité de rendre la sécurité mesurable et transparente. Les tests*

indépendants contribuent à instaurer la confiance dans la sécurité d'un produit, tant auprès des fabricants que des utilisateurs finaux ».

L'écart entre réalité technique et perception
La sécurité vérifiable constitue précisément l'une des clés permettant de relever un défi majeur du secteur. Bien que les serrures intelligentes établies sur le marché offrent un niveau de sécurité élevé, un écart subsiste souvent entre la réalité technique et la perception des consommateurs. Une récente enquête menée par Nuki auprès de ses clients montre que 44 %[1] d'entre eux considèrent les préoccupations liées à la sécurité comme l'un des principaux freins à l'achat d'une première serrure électronique. Cette tendance est également confirmée par une nouvelle étude de Parks Associates, réalisée pour le compte de la Connectivity Standards Alliance[2], qui identifie elle aussi les préoccupations liées à la confidentialité des données et à la sécurité comme des obstacles à l'adoption plus large des appareils domotiques.

« *C'est pourquoi nous accueillons explicitement le Cyber Resilience Act comme une évolution positive. Les cadres réglementaires tels que le CRA, associés à des normes industrielles fiables comme Matter et à des labels délivrés par des organismes de test indépendants tels qu'AV-TEST, contribuent à dissiper les craintes infondées. Ils permettent d'instaurer la confiance nécessaire pour que les serrures intelligentes deviennent pertinentes auprès du grand public* », explique Martin Pansy, cofondateur et CEO de Nuki.

Lorsque la conformité devient un enjeu concurrentiel
Si Nuki considère très positivement le nouveau cadre réglementaire, l'entreprise souligne également clairement ses implications économiques. La Commission européenne estime les coûts directs liés à la mise en conformité à environ 29 milliards d'euros[3], soit environ 2 % des revenus de l'industrie européenne. Toutefois, selon Martin Pansy, ce chiffre ne représente qu'une partie du problème : « *L'obligation de fournir des mises à jour de sécurité pendant cinq ans ou plus mobilise durablement les ressources des développeurs. À cela s'ajoutent des dépenses supplémentaires liées au choix des composants et des outils logiciels.* » Il s'agit d'une charge qu'une entreprise établie comme Nuki est en mesure d'absorber. Pour les start-ups, elle représente toutefois une barrière à l'entrée importante et pourrait freiner l'innovation européenne.

Dans ce contexte, Martin Pansy appelle à une surveillance stricte du marché :

« *Le CRA fixe les bons niveaux d'exigence, mais une réglementation européenne n'est jamais plus forte que son application. Des exigences strictes présentent peu d'intérêt pour les consommateurs si des produits ne répondant pas à des standards de sécurité éprouvés continuent d'entrer sur le marché européen sans contrôle. Nous avons besoin de conditions de concurrence équitables qui récompensent les entreprises responsables plutôt que celles qui cherchent à contourner la réglementation* ».

[1] Nuki Brand Survey 2025 : enquête réalisée le 30 avril 2025 auprès de 1 305 membres du Nuki Club ayant acheté une Nuki Smart Lock au cours des six mois précédant l'enquête.
[2] Parks Associates : livre blanc « Smart Home Evolution : Unlocking Value », réalisé pour le compte de la Connectivity Standards Alliance, 2025. Disponible à ce lien.
[3] Commission européenne : Commission Staff Working Document SWD (2022) 282 final, section 6.3.1, 15 septembre 2022. Disponible à ce lien.

Des visuels adaptés à une couverture éditoriale concernant ce communiqué sont disponibles ici. Vous trouverez de plus amples informations sur Nuki ainsi que des ressources visuelles générales dans notre espace presse.

À propos de Nuki Home Solutions

En 2015, une campagne de financement participatif réussie sur Kickstarter a posé les bases du succès de Nuki. Depuis, l'entreprise – fondée à Graz par les frères Martin Pansy (CEO) et Jürgen Pansy (Chief Innovation Officer) – n'a cessé de croître et compte aujourd'hui plus de 130 collaborateurs de 18 nationalités. Nuki est devenu le principal fournisseur européen de solutions d'accès intelligentes et adaptables en Europe. La marque est doublement certifiée ISO 9001 et ISO 14001, preuve de son engagement en faveur de la qualité et du respect de l'environnement. Basée en Autriche, Nuki conçoit et fabrique en Europe sa serrure connectée ainsi qu'une large gamme d'accessoires et de services, avec un objectif clair : rendre l'accès à la maison plus simple et totalement sans clé.

Contact presse & demande de sample pour test :
Agence Net-Caetera
Nathalie Lesne
Chargée de Compte
06.65.15.64.37
nl@net-caetera.fr