PRESSEMITTEILUNG

Weit über Cybersecurity Month hinaus: Sicherheit und Datenschutz von Beginn an zentrale Werte bei Nuki

Graz, am 16. Oktober 2024

- **Im Gegensatz zu anderen Smart-Lock-Anbietern: Personenbezogene und sicherheitsrelevante Daten werden nicht auf Nuki-Servern gespeichert.**
- **Transparenter Umgang mit potenziellen Sicherheitslücken: Nuki legt als einer der wenigen Hersteller von elektronischen Türschlössern Großteil von APIs offen.**
- **Neue EU-Verordnungen zu Cyber-Sicherheit und Cyber-Resilienz: Smart-Lock-Pionier aus Graz erfüllt bereits vor offiziellem Inkrafttreten wesentliche Merkmale.**

Jedes Jahr im Oktober rückt die Agentur der Europäischen Union für Cybersecurity (ENISA) das Thema der Cyber-Sicherheit in den Fokus. Ziel des European Cybersecurity Month ist es, auf Risiken sowie Gefahren im Internet aufmerksam zu machen und Kenntnisse zur IT-Sicherheit zu stärken. Smart-Lock-Pionier Nuki ist es wichtig, hier als Unternehmen Verantwortung zu übernehmen – und das nicht nur an 31 Tagen pro Jahr. *„Wir wollen einen Beitrag dazu leisten, das Vertrauen in die Sicherheit von Smart Locks zu erhöhen",* stellt Jürgen Pansy, Mitgründer und Chief Innovation Officer von Nuki, fest. Mit vielen Ansätzen und Konzepten wolle man sicherstellen, dass intelligente Türschlösser in einer zunehmend vernetzten Welt sicher bleiben.

Sicherheit und Datenschutz sind bei Nuki seit der Entwicklung des ersten Prototypen Grundprinzipien. Jürgen Pansy dazu: *„Die sichersten Daten sind unserer Meinung nach die, die man nicht aus der Hand gibt."* Deshalb sind Nuki Smart Locks seit der ersten Generation so konzipiert, dass kein obligatorisches Benutzerkonto erforderlich ist. Daten werden nicht auf den Servern von Nuki gespeichert. Alle Produkte – bis auf die Nuki Box – können ohne Account genutzt werden. Das gilt sowohl für die lokale Verwendung per Bluetooth, als auch für den Fernzugriff. In beiden Fällen werden personenbezogene und sicherheitsrelevante Daten nur lokal auf den Endgeräten und nicht auf den Servern von Nuki gespeichert. Die einzige Ausnahme bildet Nuki Web, ein Cloud-Service, für den Daten auf Nuki-Servern zwischengespeichert werden. Die Aktivierung des Dienstes ist optional und in einigen Fällen sehr praktisch: Nuki-Geräte lassen sich so übersichtlich auf dem PC oder Laptop verwalten. Ein Konto für Nuki Web ist zudem bei der Integration in einige Cloud-basierte Smart-Home-Systeme (Google Home, Amazon Alexa) Voraussetzung. Auch hier ist man bei Nuki hohen Sicherheitsstandards verpflichtet: Durch die Datenhaltung in der Europäischen Union unterliegt das Hosting strengen Datenschutz-bestimmungen, die den hohen Schutz der Userdaten gewährleisten.

In Sachen Sicherheit setzt das österreichische Unternehmen auf Ende-zu-Ende-Verschlüsselung. Dabei wird ein geheimer Schlüssel verwendet, der nur dem Sender und Empfänger bekannt ist. Gemeinsam mit starken Verschlüsselungsalgorithmen, ähnlich jenen beim Onlinebanking, und dem sogenannten Challenge-Response-Verfahren stellt man sicher, dass Abhören oder Kopieren und erneutes Wiedergeben von Sperrbefehlen an das Smart Lock unmöglich sind.

Unabhängig und extern überprüfte Produkte
Sich selbst hohe Standards in puncto Sicherheit und Datenschutz aufzuerlegen, ist eine Sache. Eine andere ist es, diese Maßstäbe von unabhängigen, externen Stellen überprüfen zu lassen. Deshalb lässt Nuki seine elektronischen Türschlösser seit der ersten Generation vom unabhängigen „AV-TEST"-Institut als „Secure IOT Produkt" zertifizieren. Dadurch wird das stetig hohe Sicherheitsniveau unter Beweis gestellt – zuletzt für die vierte Smart-Lock-Generation. Zudem erzielte das „Ultion Nuki", ein gemeinsames Produkt mit dem britischen Partner Brisant Secure explizit für den UK-Markt, eine besonders prestigeträchtige Zertifizierung. Das „BSI Kitemark for the Internet of Things" attestiert auch diesem Smart Lock physische und digitale Sicherheit höchsten Standards.

Regelmäßig aktualisierte Sicherheitsanforderungen
Risiken und Bedrohungen in puncto Cybersecurity unterliegen einem raschen Wandel. Hier kommt ein bedeutender Vorteil von Smart Locks ins Spiel: Bieten diese doch die Möglichkeit, über eine Onlineverbindung Sicherheitsupdates durchzuführen. Nutzerinnen und Nutzer erhalten automatisierte Updates und können die Sicherheitsfunktionen stets auf dem aktuellsten Stand der Technik halten. So lassen sich Sicherheitslücken schließen und neue Bedrohungen zuverlässig abwehren. Die App von Nuki prüft regelmäßig, ob Updates zur Verfügung stehen, und informiert proaktiv darüber. Jürgen Pansy dazu: *„Unsere Smart Locks sind durch ihre regelmäßige Aktualisierung und die Nutzung von Apps für Sicherheitsupdates eine moderne und sichere Lösung. Sie passen sich kontinuierlich an neue Sicherheitsanforderungen an und bieten so einen zuverlässigen Schutz."*

Offengelegte Programmierschnittstellen
Und wie transparent geht Nuki mit potenziellen Sicherheitslücken um? *„Als einer der wenigen Smart-Lock-Hersteller haben wir einen Großteil unserer APIs offengelegt. Dadurch können Entwicklerinnen und Entwickler die Sicherheitsarchitektur unseres elektronischen Türschlosses überprüfen und Schwachstellen ausschließen",* betont der Chief Innovation Officer von Nuki. Diese Transparenz stelle sicher, dass eingesetzte Technologien aktuellen Sicherheitsstandards entsprechen und vor potenziellen Angriffen schützen. Verantwortungsvolle Offenlegung (Responsible Disclosure) und sogenannte Bug-Bounty-Programme sind weitere wesentliche Elemente der Sicherheitsstrategie von Nuki. Sicherheitsexpertinnen und Sicherheitsexperten haben dadurch die Möglichkeit, Schwachstellen direkt an Nuki zu melden, ehe diese öffentlich gemacht werden. So können schnell Maßnahmen ergriffen und Sicherheitslücken geschlossen werden. Ein Bug-Bounty-Programm bietet monetäre Anreize, Schwachstellen zu finden und zu melden. All diese Schritte im Sinne der Transparenz leisten laut Pansy einen entscheidenden Beitrag zur kontinuierlichen Verbesserung der Sicherheitsmaßnahmen.

Neue EU-Richtlinien ab 2025 und 2027
Als jüngste Meilensteine für die Sicherheit von IoT-Geräten innerhalb der EU gelten der Cyber Security Act (CSA) und der Cyber Resilience Act (CRA). Die Verordnungen wurden 2023 beziehungsweise 2024 vom Parlament der Europäischen Union verabschiedet. Der Cyber Security Act kommt ab dem 1. August 2025 zur Anwendung, der Cyber Resilience Act ab 2027.

Beide Rechtsakte sollen dafür sorgen, dass IoT-Geräte in der EU sicherer werden und das Vertrauen in diese Technologie gestärkt wird. *„Bei Nuki sind wir stolz darauf, dass wir bereits heute alle wesentlichen Merkmale von CSA und CRA erfüllen",* stellt Jürgen Pansy abschließend fest.

Zu dieser Pressemitteilung passendes, hochauflösendes Bildmaterial finden Sie hier, weitere Informationen über Nuki sowie allgemeines Bildmaterial unter diesem Link.

Über Nuki Home Solutions GmbH

Nuki wurde 2014 von den Brüdern Martin Pansy (CEO) und Jürgen Pansy (Chief Innovation Officer) in Graz gegründet. Seit dem Marktstart 2016 wuchs das Unternehmen stetig und ist heute Europas führender Anbieter für smarte, nachrüstbare Zutrittslösungen. Nuki ist doppelt ISO-zertifiziert, ISO 9001 bzw. ISO 14001 bescheinigen hohe internationale Standards in Sachen Qualitäts- und Umweltmanagement-system. Aktuell beschäftigt man am Firmensitz in Graz 150 Mitarbeitende mit 18 verschiedenen Nationalitäten. Neben dem in Europa produzierten und etablierten Smart Lock sowie einem umfangreichen Zubehör- sowie Serviceangebot arbeitet Nuki mit Nachdruck an der Weiterentwicklung smarter Zutrittslösungen für eine komplett schlüssellose Zukunft.

Pressekontakt
Piabo PR:
Milena Müller-Kraus
nuki@piabo.net

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