PERSBERICHT

Beveiliging en gegevensbescherming: kernwaarden van Nuki

Graz (Oostenrijk), 16 oktober 2024

- **In tegenstelling tot andere aanbieders van slimme sloten: persoonlijke en veiligheidsrelevante gegevens worden niet opgeslagen op Nuki-servers.**
- **Transparante omgang met potentiële beveiligingsproblemen: Nuki is een van de weinige fabrikanten van elektronische deursloten die het merendeel van de API's openbaar maakt.**
- **Nieuwe EU-regelgeving op het gebied van cyberbeveiliging en cyberweerbaarheid: Smart Lock pionier uit Graz voldoet aan de belangrijkste kenmerken nog voor de officiële inwerkingtreding.**

Elk jaar in oktober richt het Europees Agentschap voor Cyberbeveiliging (ENISA) zich op het thema cyberbeveiliging. Het doel van de Europese Cybersecurity Maand is om aandacht te vestigen op risico's en gevaren op het internet en kennis over IT-beveiliging te versterken. Voor Nuki is het belangrijk om als bedrijf verantwoordelijkheid te nemen – en dat niet slechts 31 dagen per jaar. "We willen bijdragen aan het vergroten van het vertrouwen in de beveiliging van slimme sloten," zegt Jürgen Pansy, medeoprichter en Chief Innovation Officer van Nuki. Met behulp van vele benaderingen en concepten is het de bedoeling dat slimme deursloten veilig blijven, zelfs in een steeds meer verbonden wereld.

Beveiliging en gegevensbescherming zijn sinds de ontwikkeling van het eerste prototype kernwaarden bij Nuki. Jürgen Pansy zegt: "Volgens ons zijn de veiligste gegevens de gegevens die je niet uit handen geeft." Daarom zijn Nuki Smart Locks sinds de eerste generatie zo ontworpen dat er geen verplicht gebruikersaccount nodig is. Gegevens worden niet opgeslagen op de servers van Nuki. Alle producten – met uitzondering van de Nuki Box – kunnen zonder account worden gebruikt. Dit geldt zowel voor lokaal gebruik via Bluetooth als voor toegang op afstand. In beide gevallen worden persoonlijke en veiligheidsrelevante gegevens alleen lokaal op de eindapparaten opgeslagen en niet op de servers van Nuki. De enige uitzondering is Nuki Web, een cloudservice waarvoor gegevens tijdelijk op Nuki servers worden opgeslagen. Het activeren van de dienst is optioneel en in sommige gevallen zeer praktisch: Nuki-apparaten kunnen overzichtelijk op

je laptop of pc worden beheerd. Een account voor Nuki Web is ook een vereiste voor integratie in sommige cloud-gebaseerde smart home systemen (Google Home, Amazon Alexa). Ook hier zet Nuki zich in voor hoge beveiligingsstandaarden: door gegevens op te slaan in de Europese Unie, is de hosting onderworpen aan strikte gegevensbeschermingsregels die een hoog niveau van bescherming van gebruikersgegevens garanderen.

Als het gaat om beveiliging, vertrouwt het Oostenrijkse bedrijf op end-to-end encryptie. Dit houdt in dat er een geheime sleutel wordt gebruikt die alleen bekend is bij de afzender en de ontvanger. Samen met sterke versleutelingsalgoritmen, vergelijkbaar met die gebruikt bij online bankieren, en de zogenaamde challenge-response procedure, zorgt dit ervoor dat afluisteren of kopiëren en opnieuw afspelen van vergrendelingscommando's naar het slimme slot onmogelijk is.

Onafhankelijk en extern geteste producten
Het is één ding om jezelf hoge normen op te leggen op het gebied van veilige communicatie en gegevensbescherming. Het is iets anders om deze normen te laten testen door onafhankelijke, externe organisaties. Daarom heeft Nuki zijn elektronische deursloten sinds de eerste productgeneratie laten certificeren als een "Secure IOT Product" door het onafhankelijke "AV-TEST" instituut. Dit bewijst het consistent hoge beveiligingsniveau – meest recentelijk voor de vierde generatie slimme sloten. Bovendien behaalde de "Ultion Nuki", een gezamenlijk product met de Britse partner Brisant Secure expliciet voor de Britse markt, een bijzonder prestigieuze certificering. Het "BSI Kitemark for the Internet of Things" getuigt ook van de hoogste normen van fysieke en digitale beveiliging voor dit slimme slot.

Regelmatig bijgewerkte beveiligingseisen
Risico's en bedreigingen op het gebied van cyberbeveiliging veranderen snel. Hier komt een aanzienlijk voordeel van slimme sloten naar voren: ze bieden de mogelijkheid om beveiligingsupdates uit te voeren via een online verbinding. Gebruikers ontvangen automatisch updates en kunnen de beveiligingsfuncties altijd up-to-date houden met de nieuwste technologie. Dit maakt het mogelijk om beveiligingslekken te dichten en nieuwe bedreigingen betrouwbaar af te weren. De Nuki-app controleert regelmatig of er updates beschikbaar zijn en informeert gebruikers hier proactief over. Jürgen Pansy licht toe: "Onze slimme sloten zijn een moderne en veilige oplossing dankzij hun regelmatige updates en het gebruik van apps voor beveiligingsupdates. Ze passen zich continu aan nieuwe beveiligingseisen aan en bieden zo betrouwbare bescherming."

Open programmeerinterfaces
En hoe transparant gaat Nuki om met potentiële beveiligingslekken? "We zijn een van de weinige fabrikanten van slimme sloten die het merendeel van onze API's openbaar hebben gemaakt. Hierdoor kunnen ontwikkelaars de beveiligingsarchitectuur van ons elektronische deurslot controleren en kwetsbaarheden uitsluiten," benadrukt Nuki's Chief Innovation Officer. Deze transparantie zorgt ervoor dat de gebruikte technologieën voldoen aan de huidige veiligheidsnormen en beschermen tegen potentiële aanvallen. Verantwoorde openbaarmaking en bug bounty-programma's zijn verdere belangrijke elementen van Nuki's beveiligingsstrategie. Dit geeft beveiligingsexperts de mogelijkheid om kwetsbaarheden rechtstreeks aan Nuki te melden voordat ze openbaar worden gemaakt. Hierdoor kunnen snel maatregelen worden genomen en beveiligingslekken worden gedicht. Een bug bounty-programma biedt financiële beloningen om kwetsbaarheden te vinden en te melden. Volgens Pansy dragen al deze stappen op het gebied van transparantie enorm bij aan de continue verbetering van beveiligingsmaatregelen.

Nieuwe EU-richtlijnen vanaf 2025 en 2027
De meest recente mijlpalen voor de beveiliging van IoT-apparaten binnen de EU zijn de Cyber Security Act (CSA) en de Cyber Resilience Act (CRA). Deze regelgeving werd respectievelijk in 2023 en 2024 aangenomen door het Europees Parlement. De Cyber Security Act zal vanaf 1 augustus 2025 van toepassing zijn en de Cyber Resilience Act vanaf 2027. Beide wetgevingen zijn bedoeld om ervoor te zorgen dat IoT-apparaten in de EU veiliger zijn en dat het vertrouwen in deze technologie wordt versterkt. “Bij Nuki zijn we er trots op te kunnen zeggen dat we nu al voldoen aan alle belangrijke kenmerken van de CSA en CRA,” concludeert Jürgen Pansy.

Hier kunt u hoogwaardig en op dit persbericht aansluitend beeldmateriaal vinden. Meer informatie over Nuki en algemeen beeldmateriaal kunt u via deze link vinden.

Over Nuki Home Solutions GmbH
Nuki werd in 2014 in Graz (Oostenrijk) opgericht door de broers Martin Pansy (CEO) en Jürgen Pansy (Chief Innovation Officer). Het bedrijf is sinds de marktintroductie in 2016 gestaag gegroeid en is nu de toonaangevende aanbieder van slimme, achteraf in te bouwen toegangsoplossingen in Europa. Nuki is dubbel ISO-gecertificeerd. De certificeringen ISO 9001 en ISO 14001 bewijzen dat wij voldoen aan de hoogste internationale normen op het gebied van kwaliteits- en milieubeheerssystemen. Bij Nuki werken momenteel 150 mensen op het hoofdkantoor in Graz. Naast het gevestigde Smart Lock dat in Europa wordt geproduceerd en een uitgebreid assortiment accessoires en diensten, werkt Nuki hard aan de verdere ontwikkeling van slimme toegangsoplossingen voor een volledig sleutelloze toekomst.

Perscontact:
Progress Communications
Amsterdam/Antwerpen
Marie Van Gaelen & Kim Schrage
nuki@progresscommunications.eu