Maximale Sicherheit mit dem Türschloss der Zukunft

Veröffentlicht am: 21.10.2015, 22:19
Pressemitteilung von: **Profil Marketing OHG // Johannes Specht**

End-to-End-Verschlüsselung mit 32-Byte-Schlüssel: Keyturner Nuki punktet mit ausgefeiltem Sicherheitskonzept

Graz, im Oktober 2015 - Bei smarten Türschlössern ist die Sicherheit vor Hackerangriffen ein Hauptfaktor. So steht dieses Thema auch im Fokus der Entwickler von Nuki. Da der intelligente Keyturner zur Kommunikation mit der Nuki-App Bluetooth Low Energy verwendet, das selbst keine Verschlüsselungsmechanismen bietet, haben sie ein eigenes Verschlüsselungsprotokoll implementiert.

"Wir haben uns für die End-to-End-Verschlüsselung mit 32-Byte Schlüssel entschieden", erklärt Martin Pansy, Geschäftsführer von Nuki. "Dieser Schlüssel ist nur dem jeweiligen Nuki und der App bekannt. Da niemand sonst den Schlüssel kennt, ist für maximalen Schutz vor Missbrauch gesorgt - besser sogar als mit einem herkömmlichen Schlüssel."

End-to-End-Verschlüsselung
Der smarte Türöffner Nuki wird einfach auf den herkömmlichen Schließzylinder aufgesetzt und per Smartphone via App gesteuert. Damit die per Bluetooth übertragenen Daten stets sicher vor Angreifern sind, werden sie bereits vor der Übertragung von der App verschlüsselt. Erst die bereits verschlüsselten Daten werden dann per Bluetooth übertragen und beim Nuki wieder entschlüsselt. Zur Verschlüsselung der Daten wird NaCI eingesetzt, wobei ein 32-Byte-Schlüssel und 24-Byte Nonces verwendet werden.
Der geheime Schlüssel wird während des Pairings zwischen App und Nuki per Diffie-Hellman-Schlüsselaustausch erzeugt. Mit diesem mathematischen Verfahren kann auf beiden Seiten zugleich ein geheimer Schlüssel kreiert werden, ohne diesen zu übertragen.

Sicherheit bei der Nuki Bridge
Auch die Nuki Bridge wird mit diesem Verschlüsselungsprinzip gesichert. Die Bridge ermöglicht Anwendern den Status ihres Keyturners von unterwegs einzusehen und zu bedienen. Das erfordert aber auch eine dauerhafte Verbindung zu den Servern des Unternehmens und bietet damit einen potentiellen Angriffspunkt. Da jedoch sämtliche Daten, die von oder zu einem Nuki über die Server und Bridge weitergeleitet werden, mit einem Schlüssel versehen sind, der ausschließlich dem Nuki und der App bekannt sind, können sie auf dem Transportweg nicht entschlüsselt werden - auch nicht vom Server oder der Bridge.

Das Challenge-Response-Verfahren
Die Schlüssel sind am Smartphone unerreichbar für User oder andere Apps gespeichert - vorausgesetzt, das Smartphone wird nicht gerootet bzw. gejailbreaked.
Sicherheit vor Angreifern bietet das Challenge-Response-Verfahren: Hierbei wird der anderen Seite über den verschlüsselten Kanal zunächst eine sehr große Zufallszahl übermittelt (Challenge), die die andere Seite auch in der Antwort angeben muss (Response). Macht sie dies nicht, wird der Befehl abgelehnt.

"Die Sicherheit des Zuhauses unserer Kunden ist eines unserer wichtigsten Anliegen", so Martin Pansy abschließend. "Hier machen wir keinerlei Abstriche."

Nuki wird kontinierlich weiterentwickelt. Das System besteht aus dem Nuki Keyturner, der Nuki Bridge

und dem Bluetooth-Schlüsselanhänger Nuki Fob. Die Auslieferung sämtlicher Produkte ist für Februar 2016 geplant.

Weitere Informationen dazu unter www.nuki.io/de und im Onlineshop unter www.shop.nuki.io/de

Über Nuki Home Solutions
Der Türöffner Nuki ist ein einfach zu installierendes System, passend für europäische Schließzylinder. Hausschlösser lassen sich damit automatisch per Smartphone öffnen und schließen. Nuki kann per Bluetooth und WiFi gesteuert werden. Es ist seit August 2015 vorbestellbar. Die Nuki Home Solutions wurde 2014 in Graz durch Up to Eleven gegründet, einem Company Builder für mobile Produkte der Zukunft. Geschäftsführer von Up to Eleven und Nuki ist Martin Pansy.

Pressekontakt:
Profil Marketing
Florian Riener
Public Relations
Tel: + 49 (0) 531 387 33 18
Fax: + 49 (0) 531 387 33 44
E-Mail: f.riener@profil-marketing.com

Pressekontakt

Herr Johannes Specht
studentische Aushilfe

Profil Marketing OHG
Humboldstraße 21
38106 Braunschweig, Deutschland

Telefon: 0531 387 3310
E-Mail: office@profil-marketing.com
Website:

Firmenportrait

Profil Marketing ist seit über 20 Jahren die Kommunikationsagentur für IT- und HighTech-Unternehmen. Unsere Teams in Braunschweig und München vereinen Technologiekompetenz und Leidenschaft für Kommunikation. Hervorragende Kontakte zur B2C- und B2B-Presse zeichnen uns aus. Neben klassischer Pressearbeit für IT- und HighTech-Unternehmen bietet Profil Marketing Dienstleistungen in den Bereichen Online-Kommunikation, klassische Werbung, Mediaplanung und Eventmarketing.