

Ingenico Terminals im WLAN – Sicherheit ist gegeben

Produktinformation PI17-02

Seit einigen Tagen ist eine Schwachstelle in WLAN-Netzwerken bekannt geworden, die als "Key Reinstallation AttaCK" (KRACK) bezeichnet wird und den Verschlüsselungsstandard WPA2 betrifft.

Kryptographie-Experten der Ingenico-Gruppe haben die Auswirkungen untersucht. Für alle Telium-Terminals mit Zulassung an DK-Netzbetreibern ist folgendes festzustellen:

- Ein Angriffsszenario kann nur mit spezieller Technik, die sich für den gesamten Zeitraum im Bereich des jeweiligen WLAN befindet, aufgebaut werden. Massenhafte Attacken über das Internet sind somit nicht möglich.
- Experten empfehlen eine zusätzliche Verschlüsselung der Daten nach Verfahren wie SSL/TLS.
Dieses ist gegeben: Die Kommunikation vom Terminal zum Host des Netzbetreibers ist nach SSL/TLS und/oder der Bitmap-Verschlüsselung gesichert. Somit ist die gesamte Strecke kryptografisch gesichert, zusätzlich zur WLAN-Strecke selbstverständlich auch die drahtgebundene Strecke vom Router bis zum Host. Dank dieser Verschlüsselung sind sensible Daten weiterhin geschützt. Welches Verfahren jeweils eingesetzt wird, ist vom technischen Netzbetreiber vorgegeben.
- Die PIN des Karteninhabers ist zusätzlich durch eine Triple-DES-Verschlüsselung abgesichert, die nur in der Sicherheitsumgebung des Netzbetreibers decodierbar ist.
- Der gesamte Datensatz einer Transaktion ist mittels eines MACs (Message Authentication Code) gegen Manipulation geschützt, dieser ist somit manipulationssicher.
- Ingenico arbeitet permanent an Verbesserungen der Datensicherheit. So haben wir den Verschlüsselungsstandard „P2PE - Point to Point Encryption“ entsprechend der Vorgaben der internationalen Kreditkartenindustrie realisiert. Dieser wird bereits bei großen Retailern mit führenden Netzbetreibern angewendet.

Aufgrund der dargelegten Sicherheitsaspekte sehen wir keinen Grund, WLAN mit WPA2 nicht zu verwenden. Wir empfehlen, angebotene Software-Updates des WLAN-Routers vorzunehmen. Ingenico prüft weiterhin die Sicherheitsmechanismen und wird eventuell notwendige Optimierungen in kommende Software-Releases einbringen.

Für Rückfragen stehen Ihnen die bekannten Ansprechpartner gerne zur Verfügung.

Ingenico GmbH
Product Management