VeriFone GmbH | Konrad-Zuse-Str. 19-21 | 36251 Bad Hersfeld

Zur Information

12.07.2012

Berichterstattung über Angriff auf bargeldlose Kassensysteme im Einzelhandel

Sehr geehrte Damen und Herren,

VeriFone ist Weltmarktführer im Bereich elektronischer Zahlungssysteme. In dieser Eigenschaft nehmen wir die Sicherheit der Zahlungsabwicklung über unsere Terminals und der Daten sehr ernst. Wir wurden darüber informiert, dass ein unabhängiges Sicherheitsunternehmen unter Laborbedingungen Versuche unternommen hat, die Applikation von Artema Hybrid Zahlungsverkehrsterminals zu manipulieren, indem eine Fremdsoftware in den Applikationsprozessor des Terminals eingebracht wurde. Darüber hat das Sicherheitsunternehmen die Medien informiert.

Das berichtete Szenario betrifft ausschließlich das Artema Hybrid Terminal, das neben dem Applikationsprozessor zusätzlich über einen abgeschirmten Prozessor im Sicherheitsmodul verfügt. Weil dieses Modul von dem Angriff nicht betroffen ist, ist ein Ausspähen der PIN während einer erfolgreichen Kartenzahlung selbst mittels einer manipulierten Applikation nicht möglich.

In Wirklichkeit findet durch die Fremdsoftware also keine reale, sondern eine vorgetäuschte Zahlungstransaktion statt – das heißt, das Konto des Karteninhabers wird nicht belastet und der Händler bekommt kein Geld. Spätestens bei Abwicklung des normalerweise täglich durchzuführenden Kassenabschlusses wird dem Händler auffallen, dass das Terminal nicht spezifikationsgerecht arbeitet.

Hinzu kommt, dass der Angriff über die LAN-Schnittstelle nicht aus der Ferne ausgeführt werden kann, da er auf Datenpaketen beruht, die nicht über (DSL-)Router oder einen Switch übertragen werden können. Der Angreifer müsste also direkt bei dem Terminal vor Ort sein, um die Manipulation vornehmen zu können.

In der Kombination dieser Erkenntnisse ist es aus unserer Sicht daher schwer vorstellbar, mit diesem Angriff ohne Kenntnis und aktive Mitwirkung eines Händlers tatsächlich PIN und Kartendaten durch manipulierte Anzeigen im Terminaldisplay in nennenswertem Umfang auszuspähen.

Wir haben sofort nach den Behauptungen des Sicherheitsunternehmens damit begonnen, eigene Tests durchzuführen und verschiedene Sicherheitslabore damit beauftragt, uns hierbei zu unterstützen. Leider hat uns das Sicherheitsunternehmen erst diese Woche weitere notwendige Detailinformationen zur weiteren Prüfung des Sachverhaltes zur Verfügung gestellt. Zudem hatte sich das Sicherheitsunternehmen dazu entscheiden, zunächst direkt an die Medien zu gehen und hat dadurch für zusätzliche Verunsicherung gesorgt.

Wir werden den Netzbetreibern, die den Betrieb der Terminals durchführen, schnellstmöglich ein Software-Update zur Verfügung stellen, das es einem Angreifer unmöglich machen wird, Karteninhabern eine PIN-Abfrage vorzutäuschen, selbst wenn der Angreifer die vollständige Kontrolle über den Applikationsprozessor hat. Zudem wird das Software-Update die von dem Sicherheitsunternehmen in dieser Woche uns gegenüber konkretisierte Angriffsmöglichkeit der LAN-Schnittstelle beheben.

Andere Produkte der VeriFone sind von dem berichteten Angriffsszenario aufgrund abweichender Hard- und Softwarearchitektur nicht betroffen. Ebenfalls nicht betroffen ist das Artema PIN-Pad Hybrid, da es über keinen Applikationsprozessor verfügt.

Mit freundlichen Grüßen

VeriFone GmbH

Markus Hövekamp
Vorsitzender der Geschäftsführung

Norbert Albrecht
Geschäftsführer
Head of Operations