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

An
ausgewählte Kunden
der VeriFone

11.07.2012

**Weitere Informationen zum Artema Hybrid Terminal**
**Berichterstattung über Angriff auf bargeldlose Kassensysteme im Einzelhandel**

Sehr geehrte Damen und Herren,

wir nehmen Bezug auf unser Schreiben vom 04.07.2012. Mittlerweile haben wir weitere Informationen zu den Manipulationsversuchen beim Artema Hybrid Terminal erhalten, die wir gern mit Ihnen teilen möchten.

Voraussichtlich wird am Donnerstag, 12.07.2012, im ARD-Magazin „Monitor“ ein Bericht mit dem Titel „Angriff: Wie Hacker die bargeldlosen Kassensysteme im Einzelhandel knacken“ ausgestrahlt. Wir müssen davon ausgehen, dass darin ein Angriff auf ein Artema Hybrid Terminal dargestellt, da wir vom Sender WDR um entsprechende Stellungnahmen gebeten wurden.

In dem Monitor-Bericht wird nach unseren Informationen gezeigt, wie ein Terminal an eine Handelskasse angeschlossen und eine Fremdsoftware in den Applikationsprozessor des Terminals aufgespielt wird. Durch diese Software wird eine PIN-Abfrage simuliert.

Wie bereits erwähnt, erfolgt kein Zugriff auf den abgeschirmten Prozessor im Sicherheitsmodul des Terminals und auch die Integrität des Sicherheitsmoduls einschließlich der darin enthaltenen kryptographischen Schlüssel ist zu keinem Zeitpunkt gefährdet. Weil das Sicherheitsmodul 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. Spätestens bei Abwicklung des normalerweise täglich durchzuführenden Kassenabschlusses wird dem Händler auffallen, dass das Terminal nicht spezifikationsgerecht arbeitet. Dies entspricht den Ihnen mit unserem Schreiben vom 04.07.2012 übermittelten Informationen und Darstellungen.

Hinzu kommt, dass der Angriff über die LAN-Schnittstelle nicht aus der Ferne ausgeführt werden kann, da er auf sogenannten ARP-Paketen beruht, die nicht über (DSL-)Router oder einen Switch übertragen werden können. Der Angreifer muss 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 in nennenswertem Umfang auszuspähen.

Wir nehmen die Sicherheit der Terminals und der Daten sehr ernst. Daher haben wir direkt 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 genauen Prüfung des Sachverhaltes übergeben.

Wir werden Ihnen 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 Verwundbarkeit der LAN-Schnittstelle beheben.

Aufgrund der avisierten Berichterstattung der ARD und sich möglicherweise anschließender Medienberichte ist es möglich, dass Ihr Kassenpersonal von Karteninhabern mit Fragen oder Anmerkungen zum in den Medienbeiträgen gezeigten Artema Hybrid konfrontiert wird. Gern können Sie dieses Schreiben als Grundlage für die Information Ihrer Mitarbeiterinnen und Mitarbeiter verwenden.

Bitte kontaktieren Sie uns, wenn wir Sie mit weiteren Informationen oder Argumentationshilfen unterstützen können.

Einstweilen bedanken wir uns bei Ihnen für Ihr Vertrauen und für die Zusammenarbeit.

Mit freundlichen Grüßen

VeriFone GmbH

Markus Hövekamp
Vorsitzender der Geschäftsführung

Norbert Albrecht
Geschäftsführer
Head of Operations