Quelle: futurezone.at
Adresse: http://futurezone.at/digital-life/hacker-kopieren-kreditkarten-im-geschaeft-per-bezahl-terminal/214.205.003
Datum: 07.08.2016, 15:41

SCHWACHSTELLE

Hacker kopieren Kreditkarten per Bezahl-Terminal im Geschäft

Security-Forscher haben eine Schwachstelle entdeckt, mit der Kreditkartendaten und der PIN-Code in Geschäften abgegriffen werden kann.

Laut den Forschern übertragen viele POS-Terminals die Daten ungesichert zum Computer mit der Zahlungssoftware (Symbolbild) - Foto: Visa

Der EMV-Standard galt bisher als relativ sicher. Ein Chip auf der Kredit- und Bankomatkarte ersetzt den Magnetstreifen, statt unterschrieben wird ein PIN-Code eingegeben, um die Zahlung zu autorisieren. In Europa ist dieses Verfahren seit Jahren üblich und kommt in Geschäften bei POS-Terminals zum Einsatz.

Bei der Black Hat Konferenz, die diese Woche in Las Vegas stattgefunden hat, haben jetzt zwei Security-Forscher gezeigt, wie die Terminals zum Abgreifen der Kreditkartendaten genutzt werden können. Die Forscher, Nir Valtman und Patrick Watson, arbeiten für NCR, einen der Marktführer für Bankomaten und bargeldlose Bezahlsysteme, wie Softpedia berichtet.

Die Schwachstelle, die sie entdeckt haben, liegt zwischen den Terminals und der dazugehörigen Software. Die typischen POS-Terminals bestehen aus Display, Kartenleser und Tasten zur Eingabe des PIN-Codes. Die Daten vom Kartenleser werden unverschlüsselt zur Software übertragen, die meist auf einem Computer in der Nähe des Terminals installiert ist.

Schnüffel-Hardware

Je nach Gerät erfolgt die Übertragung per Ethernet-Kabel oder drahtlos. Die Forscher haben für ihre Demonstration einen Raspberry Pi zwischen Terminal und Notebook mit der Software gehängt, auf dem ein Programm zum Abgreifen des Datenverkehrs installiert war. Laut den Forschern könnte man dies auch mit deutlich kleineren Geräten machen, die kaum auffallen, wenn sie richtig positioniert werden.

Die Geräte könnten etwa von Insidern oder Personen installiert werden, die sich als Techniker ausgeben. Durch eine manipulierte DLL-Datei könnten Hacker auch die Software manipulieren, um die unverschlüsselten Daten weiterzuleiten. Vorausgesetzt, sie verschaffen sich aus der Ferne Zugriff auf den Computer, auf dem die Software installiert ist.

Doppelte PIN-Eingabe

Die Kreditkartendaten alleine bringen Cyberkriminellen nicht allzu viel, weshalb die Forscher auch gleich demonstriert haben, wie sie an den PIN-Code kommen können. Die PIN-Eingabe am Terminal zur Bestätigung der Zahlung verschlüsselt. Durch eine manipulierte DLL ist es aber möglich, nach der eigentlichen PIN-Eingabe den Kunden zur erneuten Eingabe aufzufordern. Diese wird dann unverschlüsselt gesendet.

Laut den Forschern schöpfen die meisten Kunden hier keinen Verdacht, weil sie annehmen, sie hätten den PIN beim ersten Mal falsch eingetippt. Sie empfehlen aktiv darauf zu achten, da eine erneute Eingabeaufforderung des PINs fast immer auf ein manipuliertes Gerät hindeutet.

Den Herstellern der POS-Terminals empfehlen sie eine Point-to-Point Encryption (P2PE) zu implementieren. Ist die Hardware zu alt für P2PE, sollte zumindest die Datenübertragung zwischen Terminal und Software mittels TLS gesichert werden.

Die Terminals welcher Hersteller die Daten ungesichert übertragen, wollten die Forscher nicht verraten. Es seien jedoch sehr viele Geräte getroffen. Die Hersteller wurden von den Forschern über die Schwachstelle informiert.

(FUTUREZONE) ERSTELLT AM 07.08.2016, 15:23

Stichworte: Hacker, Kreditkarte,