AUTOMATEN SEITZ
since 1963

Anschrift

Datum: 02.02.2010
Unser Zeichen: SM/AF/MH
Unsere Tel. Nr.: 089 / 427 35 - 0
Unsere Fax Nr.: 089 / 427 35 - 111

Ihre Zeichen:
Ihre Nachricht:
Ihre Tel. Nr.:
Ihre Fax Nr.:

Sicherheitsaspekte LEGIC prime

Sehr geehrter Kunde,

nach Auswertung der uns vorliegenden Informationen (Produktmitteilung Fa. LEGIC vom Januar 2010, Tagungsinformationen vom 26. Kongress des CCC und von Heise Online „26C3: Sicherheitssystem der RFID…"), können wir Stand heute folgendes zur Einschätzung der Lage beitragen.

Von welcher Technologie ist die Rede?

Betroffen ist der LEGIC prime Standard in der MIM22, MIM256 und MIM1024 Variante. Durch verschiedene hard- und softwaretechnische Methoden (incl. des Abtragens einzelner Schichten eines Chips), wurde der Chipaufbau (incl. der Sicherheitslogik) ermittelt. Weiterführend wurde die Verschlüsselung bzw. Schutzmechanismen zwischen Karte und Leser analysiert. Dazu waren und sind Hardware, Tools und spezielles IT-Know-how notwendig.

Welche Auswirkungen kann dies haben?

Für den ungünstigsten Fall, können damit Karten dupliziert und/oder Dateninhalte verändert werden. Nach den uns vorliegenden Informationen ist die Chipseriennummer (UID) davon nicht betroffen, d.h. die UID ist eindeutig.

Wie kann ein Missbrauch bei kopierten Karten festgestellt werden?

Unsere Systeme führen mit jeder Einzeltransaktion auch einen Vorgangszähler (VGZ) mit. Wird eine LEGIC prime Karte dupliziert, kann dies über einen Sonderbericht, der nach eklatanten Vorgangszählersprüngen auswertet, festgestellt werden. Es gibt in diesem Fall zwei gleiche Karten, mit gleicher Kartennummer, die in den Start- und Endsalden Auffälligkeiten aufweisen. Bei Verdachtsfällen, kann die Karte über eine Sperrdatei für weitere Bezahlvorgänge gesperrt werden.

Automaten Seitz · Vertrieb und Kundendienst GmbH
Postfach 82 01 05, 81801 München · Telefon: 0 89 / 4 27 35 - 0 · Telefax: 0 89 / 4 27 35 - 111 · Schatzbogen 49, 81829 München
Email: info@automaten-seitz.de · Web: www.automaten-seitz.de

Geschäftsführer: Andrea Seitz-Maier · Amtsgericht München HRB 94264
Postbank München, BLZ 700 100 80, Konto 1659 60-809 · Stadtsparkasse München, BLZ 701 500 00, Konto 73 080 · VR Bank München Land eG, BLZ 701 664 86, Konto 292 65 98

Ist eine Datenmanipulation möglich?

Eine Manipulation ist nur mit tieferem Verständnis und genauer Kenntnis

- über den Kartenaufbau (an welchem Byte steht welche Information),
- über Anzahl und Position der Speicherblöcke
- über den Algorithmus der Checksummenbildung

möglich.

Diese aufgeführten Mechanismen sind geschützt. Eine Manipulation ohne diese Kenntnisse, würde also mit hoher Wahrscheinlichkeit nicht ohne Fehler stattfinden. Eine Plausibilitätsprüfung während dem Bezahlvorgang weist diese Karte sofort ab.

Sollten alle Hürden überwunden sein, und z.B. gezielt ein Euro Betrag „korrekt" manipuliert worden sein, dann ist dies bei einem Vergleich durch das mitgeführte Schattenkonto auf der Datenbankseite (doppelte Buchführung) im Nachhinein feststellbar.

Gibt es zusätzliche Sicherheitsmaßnahmen?

Automaten Seitz deckt jetzt schon Kartenmanipulationen mit der UID auf. Voraussetzung ist hierzu ein aktueller Softwarestand.

Automaten Seitz erstellt ein weiteres Sicherheitsupgrade. Die UID wird in eine erweiterte Identitäts- und Plausibilitätsprüfung involviert. Eine zusätzliche Verschlüsselung der Daten auf der Karte wird integriert werden. Ein entsprechendes Upgrade wird zeitnah zur Verfügung gestellt. Nach den Freigabetests können wir Ihnen den Liefertermin nennen.

Welche weiterführende Empfehlung gibt es?

Die jüngere und modernere LEGIC Advant Technologie hat einen höheren Sicherheitsstandard wie die LEGIC prime Variante. Verschlüsselungsmechanismus und Sicherheitsmerkmale sind weitergehend.

Alternativ dazu gibt es die MIFARE DESFire Technologie. Diese weist ebenso einen höheren Sicherheitsstandard als LEGIC prime auf. Derzeit aktuelle Verschlüsselungsmechanismen sind integriert. Die Karte selbst beinhaltet einen Prozessor, welcher z.B. autark Spiegelspeicher führt.

Für die Umstellung auf diese Technologien müssen die Leser geprüft und ggf. aktualisiert/ausgetauscht und ein Softwareupgrade vorgenommen werden. Die LEGIC Advant Leser verhalten sich abwärtskompatibel, d.h. LEGIC prime Medien (z.B. Karten) funktionieren auch mit LEGIC Advant Lesern und Software. Dies ermöglicht eine schrittweise Umstellung auf LEGIC Advant Medien.

AUTOMATEN SEITZ
since 1963

Möchte man die MIFARE DESFire Technologie einsetzen, müssen die LEGIC prime Karten gegen MIFARE DESFire Karten ausgetauscht werden. Der Austausch der Leser in MIFARE DESFire Modelle muss zu einem Stichtag vollzogen werden. Es gibt keinen Parallelbetrieb der Systeme, da sich die Technologien grundlegend unterscheiden.

Zusammenfassung

Eine massive und akute Bedrohung oder unauffällige Massenmanipulation sehen wir im Moment nicht. Dazu sind zusätzliche Hardware und spezielles, tiefes IT-Know-how notwendig. Angriffe und Manipulationen auf das System können wir nicht ausschließen. Daher bitten wir Sie in Ihrem Interesse, dass Sie die Systemberichte beobachten und Datenanalysen durchführen um eventuelle Unregelmäßigkeiten rechtzeitig zu erkennen. Das Hintergrundsystem von Automaten Seitz bietet zusätzliche Sicherheiten und Prüfungsmöglichkeiten. Allerdings empfehlen wir als Vorsichtsmaßnahme den Einsatz des Upgrades.

Mittelfristig sollte der Umstieg auf neuere Technologie wie LEGIC Advant und MIFARE DESFire in Betracht gezogen werden.

Gerne erstellen wir in Ihrem Auftrag eine Systemanalyse und geben Ihnen Empfehlungen für weitere Sicherheitsprüfungen.

Mit freundlichen Grüßen

AUTOMATEN SEITZ GmbH

A. Seitz-M

Andrea Seitz-Maier
Geschäftsführerin