

ZENTRALER KREDITAUSSCHUSS

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN • BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN • DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER PFANDBRIEFBANKEN E.V. BERLIN

Lessons learned aus dem “2010-Problem” - Business Continuity Management in Chipkartensystemen

Berlin, 14.04.2010

1 Einleitung

Mit Beginn des Jahres 2010 wurden viele Inhaber deutscher Debit- und Kreditkarten Opfer eines unerwarteten Ereignisses: Ihre Karten wurden an vielen POS-Kassen und Geldautomaten plötzlich nicht mehr akzeptiert. Was war passiert?

Betroffen waren Karten mit einem so genannten EMV-Chip. EMV ist ein Standard für Chipkartentransaktionen, der von den internationalen Zahlungssystemen Eurocard, MasterCard und Visa entwickelt worden ist und bis Ende 2010 auf allen Karten und an allen POS-Terminals und Geldautomaten in Europa eingeführt wird. Ein Programmierfehler in Chipkarten einer bestimmten Produktlinie des namhaften Herstellers Gemalto hatte dazu geführt, dass eben diese Karten an EMV-fähigen Terminals ab dem 1. Januar 2010 einen "Kartenfehler" meldeten und die Transaktion abgebrochen wurde. Alle anderen im Umlauf befindlichen Karten zeigten dagegen keinerlei Auffälligkeiten.

Aufgrund des Programmierfehlers hielten die betroffenen Chipkarten ein Transaktionsdatum ab dem 1. Januar 2010 für fehlerhaft. Eine zeitnahe Analyse der Kartensoftware zeigte, dass der Programmierfehler in der Karte durch die Anordnung bestimmter Daten im Chip der Karte, die ihrerseits mit der Datumsverarbeitung der Karten in keinem Zusammenhang stehen, aktiviert oder deaktiviert wird.

Diese Verkettung verschiedener, grundsätzlich voneinander unabhängiger Daten ist mit einer verborgenen Softwarefunktion vergleichbar, die ein Programm nur in ganz bestimmten Fällen abstürzen lässt. In dem aktuellen Fall verursacht eine verborgene Softwarefunktion in Verbindung mit einer speziellen Konfiguration von Kartendaten und bei Erreichen eines bestimmten Datums den Fehler.

Wenn aber die Ausführung der verborgenen Softwarefunktion durch eine geeignete Umkonfiguration von Kartendaten verhindert wird, funktioniert die eigentliche Transaktionsverarbeitung durch die Karte auch mit Transaktionsdaten ab 2010 wieder völlig korrekt, die Fehler verursachende Interdependenz wird aufgehoben. Es ist also möglich, das Wirksamwerden des Fehlers durch Umsortierung einiger weniger, nicht sicherheitskritischer Daten der Chipkarte grundsätzlich zu verhindern.

ZKA-Federführer

Deutscher Sparkassen- und Giroverband
Charlottenstr. 47 • 10117 Berlin • Tel.: (030) 20 225 5115 • Fax: (030) 20 225 5119 • presse@dsgv.de
www.dsgv.de

Zentraler Kreditausschuss im Internet: www.zka.de

Der aufgetretene Fehler bei deutschen Chipkarten ist somit in keiner Weise mit dem typischen "Jahr 2000"-Fehler vergleichbar, der systembedingt mit dem Jahrtausendwechsel auftreten konnte. Es handelte sich vielmehr um einen von der eigentlichen Datumsverarbeitung unabhängig auftretenden Programmierfehler. Teilweise öffentlich vermutete Begründungen, die Jahreszahl der Karte sei einstellig bzw. die Jahreszahl "10" würde intern durch die Karte als "16" interpretiert, entsprechen nicht den Tatsachen. Auch ist die in Medien häufig genutzte Etikettierung des Fehlers als "2010-Problem" unter technischen Gesichtspunkten nicht korrekt – zutreffend ist nur, dass der Fehler erst mit dem Beginn des Jahres 2010 wirksam geworden ist.

Sehr schnell konnte der Zentrale Kreditausschuss feststellen, dass von dem Fehler etwa 30 Millionen deutsche Chipkarten betroffen waren – keine Karten der neuesten Generation, sondern ältere Karten, die bereits seit vielen Jahren im Einsatz sind.

Bei einer derart großen Zahl betroffener Karten ist die Änderung der ausgegebenen Chipkarten eine bedeutend schnellere Lösung als ein kompletter Austausch und zudem bequemer für den Karteninhaber, da dieser sich keine neue Geheimnummer merken muss. Aber auch eine „Update“-Lösung für Karten im Feld benötigt bis zur Verfügbarkeit für den betroffenen Karteninhaber Zeit für Entwicklung, Test, Sicherheitsbegutachtung und das Ausrollen in die IT-Systeme der Kreditinstitute.

Um den Karteninhabern bis zur abschließenden Problembeseitigung die Möglichkeit zu geben, ihre Karten weitgehend, also zumindest im Inland, zu nutzen, waren weitere sofortige Maßnahmen zur Wiederherstellung der Akzeptanz erforderlich.

Damit sorgte ein „kleiner“ Softwarefehler in der Chipkartensoftware eines Herstellers für einen kritischen Anwendungsfall für ein schnelles und wirksames Business Continuity Management in einem Chipkartensystem und das in einer weltweit bislang nicht aufgetretenen Größenordnung.

2 Sofortmaßnahmen - Wiederherstellung der Akzeptanz im nationalen System innerhalb einer Woche

Die deutsche Kreditwirtschaft war in der Lage, auf diese Notfallsituation innerhalb kürzester Zeit in ihren Zahlungssystemen zu reagieren. Durch Ausnutzung der in den kreditwirtschaftlichen Spezifikationen vorgesehenen Möglichkeiten der Konfiguration von Terminals konnte die Akzeptanz der fehlerhaften Karten an allen Geldautomaten des Deutschen Geldautomatensystems und an allen electronic cash-Terminals innerhalb einer Woche nach Auftreten des Fehlers wieder hergestellt werden.

Konfiguration bedeutet, dass durch einen Daten-Download der Ablauf einer Transaktion in Geldautomaten und electronic cash-Terminals so verändert wird, dass die Karten wieder akzeptiert werden können. Es war jedoch aufgrund der Flexibilität der benutzten Terminal-Infrastruktur nicht erforderlich, die Anwendungs-Software in den Terminals zu ändern.

An Geldautomaten wurde der Ablauf dahingehend verändert, dass immer dann, wenn der Kartenfehler auftrat, auf den Magnetstreifen der Karte „zurückgefallen“ wurde (Fallback). Das Sicherheitsniveau der Transaktionen blieb dabei unverändert hoch, da zur Überprüfung der Echtheit der Karten auf das von allen Karten und allen Geldautomaten unterstützte MM-

Sicherheitssystem zurückgegriffen werden konnte. So war es trotz Notfallprogramm unverändert nicht möglich, mit gefälschten Karten an Geldautomaten zu verfügen.

An electronic cash-Terminals wurde der Ablauf dahingehend geändert, dass auf die in den betroffenen Chipkarten noch vorhandene alte nationale electronic cash-Chipanwendung umgeschaltet und somit die fehlerhaft arbeitende EMV-Anwendung der Chipkarte nicht mehr benutzt wurde. Da die Umstellung der electronic cash-Terminals auf den EMV-Standard erst 2010 abgeschlossen wird, unterstützen die meisten Terminals noch die „alte“ electronic cash-Chipanwendung, so dass in diesen Fällen – trotz Chipkartenfehler – weiterhin der Chip für die Abwicklung der Kartentransaktion genutzt werden konnte. Nur an den sehr wenigen electronic cash-Terminals, die schon so weit umgerüstet waren, dass sie die bisherige nationale electronic cash-Chipanwendung nicht mehr unterstützen, wurden die fehlerhaften Karten über den Magnetstreifen der Karte akzeptiert. Die Geldautomaten wurden auf eine fallweise Magnetstreifenverarbeitung mit integrierter Kartenechtheitsprüfung umgestellt.

Es erfolgte also nicht - wie mitunter in der Presse vereinfacht dargestellt - ein „Umschalten“ vom Chip auf den Magnetstreifen. Vielmehr wurde zur Erhaltung der Systemvorgaben sichergestellt, dass nur für die fehlerhaften Karten ein alternatives, möglichst sicheres Abwicklungsverfahren zur Anwendung kommt. Wann immer möglich, wurde daher im nationalen Umfeld auf eine andere Chipanwendung „umgeschaltet“. Hierzu war es nötig, innerhalb kürzester Zeit einen Daten-Download für knapp 57.000 Geldautomaten und über 250.000 electronic cash-Terminals durchzuführen.

Nachdem die ersten Meldungen über den Fehler am 2. Januar auftraten, war die überwiegende Zahl der Geldautomaten in Deutschland bereits am Abend des Folgetages umgestellt. Bis zum 8. Januar war die Umstellung komplett vollzogen.

Am Morgen des 4. Januar 2010, dem ersten Arbeitstag im neuen Jahr, wurden alle electronic cash-Netzbetreiber durch den Zentralen Kreditausschuss nach erster Problemanalyse informiert und es wurde eine Umkonfiguration der Terminals als sinnvolle Sofortmaßnahme festgelegt. Diese konzertierte Aktion war nur möglich, weil die electronic cash-Terminals gemäß den Vorgaben der deutschen Kreditwirtschaft ein standardisiertes Verfahren zum Daten-Download neuer Konfigurationen unterstützen. Im Laufe des gleichen Tages wurde die neue Konfiguration getestet und abgenommen. Die electronic cash-Netzbetreiber stellten daraufhin die neue Konfiguration umgehend für ihre Terminals im Handel zum Download bereit. Bis zum 8. Januar hatten alle aktiven electronic cash-Terminals diese neuen Konfigurationsdaten über die im Rahmen des electronic-cash-Verfahrens vorgeschriebene durchgehende online-Anbindung zum Netzbetreiber erhalten.

Damit war die Akzeptanz der fehlerhaften Karten an allen Geldautomaten und electronic cash-Terminals in Deutschland wieder gewährleistet.

Leider standen für die internationalen Zahlungssysteme, und damit für die Kunden, die im Ausland mit ihren betroffenen Karten verfügen wollten, keine entsprechenden systemweiten Möglichkeiten zur Anpassung von Terminalkonfigurationen zur Verfügung. Es war deshalb für die deutsche Kreditwirtschaft nicht möglich, die Akzeptanz der fehlerhaften Karten in den internationalen Zahlungssystemen in gleicher Weise und unmittelbar wieder herzustellen.

Um die Akzeptanz der fehlerhaften Karten auch im Rahmen der internationalen Zahlungssysteme wieder vollständig herzustellen, ist die Anpassung der betroffenen Karten oder ein Kartentausch erforderlich. Um die Einschränkungen für die Karteninhaber im Ausland so gering wie möglich zu halten, war es notwendig, eine gemeinschaftliche kreditwirtschaftliche Lösung zu schaffen, die eine Änderung der Datenelemente in der Karte per Update sehr kurzfristig ermöglicht. Sie musste der Kontrolle des kartenausgebenden Instituts unterliegen und das sehr hohe Sicherheitsniveau der deutschen Zahlungssysteme einhalten.

3 Update-System zur Anpassung von Datenelementen in der Karte

Die Möglichkeit einer sicheren Anpassung von Daten in bereits ausgegebenen Chipkarten ist ein wichtiger Vorteil gegenüber reinen Magnetstreifenkarten. Der Mikroprozessor in der Karte gestattet es, geschützt durch kryptografische Verfahren Daten der Chipkarte zu verändern. So kann man sich während einer Transaktion von der Echtheit einer Karte überzeugen, den PIN-Fehlbedienungszähler pflegen oder Verfügungslimits in der Karte im Rahmen einer sicheren Online-Kommunikation zwischen Karte und Hintergrundsystem des Kartenausgebers ändern. Ein anderer typischer Fall der Online-Änderung von Daten der Chipkarte ist das Aufladen von GeldKarte-Guthaben. Das geladene Guthaben wird in der Karte gespeichert und kann anschließend offline „verbraucht“ werden.

Chipkarte und Hintergrundsystem des Kartenausgebers teilen sich kryptografische Schlüssel, die es beiden Instanzen erlaubt, zweifelsfrei festzustellen, ob eine übermittelte Nachricht vom jeweils anderen Partner stammt bzw. ob Inhalte dieser Nachricht verändert worden sind. Erst Chipkarten machen es möglich, dass der Kartenemittent sicher mit seiner bereits ausgegebenen Karte „sprechen“ kann und dass dabei jede Manipulation durch Dritte in der Kommunikation sofort erkannt werden würde.

Durch Nutzung dieser in der Praxis vorhandenen und im täglichen Betrieb genutzten sicheren Anpassungsmechanismen konnten die betroffenen Chipkarten auch an ausländischen Terminals wieder voll funktionsfähig gemacht werden.

Bei der Analyse des Fehlers war festgestellt worden, dass es nur dann zu einem Abbruch der Transaktion kam, wenn bestimmte Datenelemente in einem Datenfeld der Karte in einer ganz bestimmten Weise sortiert waren. Hierbei handelt es sich um ein Datenfeld, mit dem die Karte dem Terminal anzeigt, in welcher Reihenfolge Transaktionsdaten, wie z.B. der Transaktionsbetrag, das Datum oder die Währung der Transaktion vom Terminal an die Karte zu übergeben sind. Bei einer anderen Sortierung der Datenelemente in dem Datenfeld wirkte sich der Software-Fehler hingegen nicht mehr aus. Daher lag die naheliegende Lösung des Softwareproblems in einer Umsortierung der Datenelemente. Anhand von Tests konnte dann gezeigt werden, dass diese Einschätzung korrekt war, der Fehler verschwand.

Leider zeigte eine weiterführende Analyse auch, dass eine Umsortierung dieser Datenelemente („Update“) nicht im Rahmen einer normalen Online-Autorisierung vorgenommen werden konnte, zum Beispiel im Zuge einer Verfügung am Geldautomaten. Da der Fehler im Transaktionsablauf bereits vor dem Start einer Online-Transaktion zum Tragen kam, schied diese Möglichkeit aus. Es war also erforderlich, für das Karten-Update einen speziellen und sicheren gesonderten Transaktionsablauf in den kreditwirtschaftlichen Systemen zu definieren.

Innerhalb von zwei Wochen nach erstmaligem Auftreten des Fehlers stand bereits ein Testsystem zur Verfügung, mit dem von dem Fehler betroffene Karten (zunächst im Pilottest) erfolgreich angepasst wurden. Sie waren danach wieder voll funktionsfähig.

Auf der Grundlage der Ergebnisse des Pilottests erfolgte die Vorbereitung für einen flächendeckenden Einsatz des speziellen Ablaufs zur abgesicherten Umsortierung der relevanten Datenelemente im kreditwirtschaftlichen System. Die kartenausgebenden Institute haben hierbei die Möglichkeit, ihren Kunden eine „Reparatur“ ihrer Karten entweder an speziellen Terminals im Schalterbereich oder an Kundenselbstbedienungsterminals, vornehmlich Geldautomaten, anzubieten. Die Aktualisierung der Daten der Chipkarte erfolgt für den Karteninhaber nahezu unmerklich und benötigt nur Bruchteile von Sekunden. Dem Kunden wird danach der Erfolg der Anpassung angezeigt.

Da die Sicherheitsmechanismen der verschiedenen von der Karte unterstützten Zahlungssysteme durch die Umsortierung der Datenelemente nicht beeinflusst werden, ist es auch nicht zwingend erforderlich, dass sich der Karteninhaber bei der „Reparatur“ zuerst mit seiner PIN authentisiert. Dies ist wichtig, um auch die von dem Fehler betroffenen Kreditkarten anpassen zu können, bei denen die Karteninhaber häufig gar nicht über eine PIN verfügen.

Das erfolgreich getestete System wird seit Ende Januar, nach und nach flächendeckend für eine Korrektur der Daten in den von dem Fehler betroffenen Chipkarten genutzt. Mit dann wieder voll funktionsfähigen Chipkarten muss vom Kunden auch im Ausland keine Rückweisung mehr befürchtet werden.

4 Lessons learned

Der in Deutschland aufgetretene Fall ist der bisher größte Fall eines Herstellerfehlers in der Chipkartensoftware in Deutschland, der erst nach der Kartenausgabe festgestellt wurde und massive Folgen für die Kartenakzeptanz hatte. Selbstverständlich wurden als erste Erkenntnis daraus in allen Testverfahren zusätzliche Datumstests aufgenommen, die nunmehr jedes Transaktionsdatum während des Lebenszyklus einer Chipkarte testen. Trotzdem muss man sich darüber im Klaren sein, dass aufgrund der Komplexität der Chipkartentechnik ein Test aller möglichen Belegungen aller variablen Datenelemente einschließlich aller denkbaren Kombinationen von Belegungen dieser Datenfelder letztlich nicht vollumfänglich möglich ist. Insofern kann auch für die Zukunft niemals vollständig ausgeschlossen werden, dass es zu Fehlern in Chipkartensystemen kommt, die auch – wie in diesem Fall - erst deutlich nach Ausgabe der Karten an die Karteninhaber auftreten können.

Wichtig ist die Feststellung, dass die von der deutschen Kreditwirtschaft ergriffenen gemeinschaftlichen Maßnahmen zur Fortführung des Betriebs ihrer Zahlungssysteme in diesem Krisenfall sehr gut funktioniert haben. Die Akzeptanz aller Karten an allen in den Zahlungssystemen der deutschen Kreditwirtschaft betriebenen Terminals war innerhalb sehr kurzer Zeit wieder erreicht. Das Vertrauen der Kunden in die Karte bleibt gewahrt. Gleichzeitig hat sich auch der Systemdesignansatz bewährt, dass die deutsche Kreditwirtschaft sehr detaillierte Vorgaben für das Chipkartenbetriebssystem vorsieht. Dies hat es ermöglicht, wahrscheinlich erstmals in der Welt und in dieser Größenordnung, für eine sehr große Zahl von Karten eine „Reparatur“ im Feld durchzuführen. Erst dadurch kann dem Karteninhabern die Unbequemlichkeit eines Kartenaustauschs erspart werden.

Sicherlich ist sorgfältig zu prüfen, wie die Reaktionszeiten in der Krisenbewältigung noch weiter verkürzt werden können. Man kann aber schon jetzt die Schlussfolgerung ziehen, dass die zur Umsortierung der Daten per Update in den fehlerhaften Chipkarten entwickelte kreditwirtschaftliche Infrastruktur auch in der Zukunft eine wichtige Notfalllösung sein kann.

Der aktuelle Fall hat aber auch gezeigt, dass in den internationalen Zahlungssystemen bislang keine vergleichbaren systemweiten Reaktionsmöglichkeiten zur Verfügung stehen.

Ingesamt zu fordern – insbesondere auf Ebene des Kartensystembetreibers – sind daher durchgehende praktikable Lösungen für das Business Continuity Management, denn im Zweifel ist ein kurzfristiger großflächiger Austausch von Chipkarten weder logistisch noch wirtschaftlich durch kartenausgebende Institute darstellbar. Für kleinere Portfolien ist und bleibt ein Kartentausch eine Option.

Die deutsche Kreditwirtschaft hat - wie oben dargestellt - für den Krisenfall bereits eine Reihe von guten und ausbaufähigen Ansätzen entwickelt, die im aktuellen Fall zur schnellen Problemlösung erfolgreich genutzt werden konnten. Im Interesse der kartenausgebenden Institute ist es sinnvoll, aufbauend auf den Erfahrungen in den Zahlungssystemen der deutschen Kreditwirtschaft, auch auf internationaler Ebene über entsprechende interoperable Ansätze nachzudenken.