Je näher am Kern, desto restriktiver die Maßnahmen

Nicht nur die Nutzung, sondern auch die Produktion von Identifikationskarten unterliegt strengen Sicherheitsbestimmungen/Das Beispiel ComCard

Von Swen Hopfe

Die Welt des zweiten Jahrtausends setzt nicht alles, aber doch vieles auf eine Karte. Auch wenn sich berührungslos funktionierende Identifikationsverfahren, etwa RFID, auch in andere Medien integrieren lassen, so ist die Plastikkarte für die unterschiedlichsten Anwendungen immer noch weit verbreitet. Tatsächlich verrät uns im Prinzip schon allein die nach der Norm ISO 7810 für Identitätsdokumente definierte Größe, dass wir hier ein Stück Plastik in der Hand halten, dessen Verlust oder Missbrauch schwerwiegende Folgen haben kann.

Die genannte Norm legt vier unterschiedliche Größen für Karten fest. Das Format „ID-1" (85,60 x 53,98 mm) gilt in der Regel für Bank-, Debit-, Kreditkarten und Führerscheine. Der deutsche Personalausweis entspricht der Größe „ID-2" (105 x 74 mm = DIN A7). An „ID-3" (125 x 88 mm) orientieren sich weltweit alle Reisepässe. Und für die kleine SIM-Karte in Mobiltelefonen gibt es „ID-000" mit 125 x 88 mm. Ihnen allen ist vor allem eines gemeinsam: Sie enthalten entweder einmalige, wichtige Informationen, die nicht in die Hände Unbefugter gelangen dürfen. Oder sie weisen den Ausweisinhaber als denjenigen aus, der er ist, und dürfen deshalb als Ganzes nicht an Betrüger geraten.

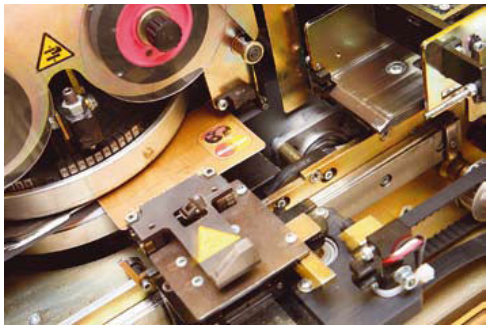
Die Produktion im Spannungsfeld

Darüber, dass über den sicheren Umgang der Inhaber mit ihren Bankkarten oft und viel die Rede ist, gerät meist in Vergessenheit, dass auch für die Produktion dieser Karten weitaus höhere Sicherheitsanforderungen gestellt werden als – beispielsweise – bei Motiv- oder Geschenkkarten. Nicht auszudenken, wenn jemand „mal eben" den Chip auf der Kreditkarte so programmiert, dass er Unberechtigten die PIN freigibt.

Das stellt auch die ComCard GmbH vor große Sicherheitsherausforderungen. Das Unternehmen fertigt und personalisiert „ID-1"-Chipkarten für den Zahlungsverkehr, das Gesundheitswesen, zur Identifikation und Kundenbindung. Der Kundenkreis umfasst weltweit Kreditinstitute, Versicherungen sowie Handels- und Systemhäuser. Auch ComCard setzt auf die elektronische Zutrittskontrolle zum Schutz seiner Produktionsumgebung. Immerhin bewegt man sich damit sozusagen im ureigensten Kompetenzumfeld. Solche Kontrollen können mittels sehr unterschiedlicher Formen von physischen und logischen Mechanismen (Berechtigungs-Token, PINs und biometrische Erkennungsverfahren, Kameras, Alarmmelder usw.) erfolgen.

Im Informationszeitalter hat sich aber auch bei ComCard der Fokus von überwachten Ein- und Ausgängen hin zu integrierten Sicherheitskonzepten verschoben. Sie garantieren, dass von Beginn der Wertschöpfung bis hin zum fertigen Produkt das notwendige Maß an Sicherheit vor Zugriff und Manipulation gegeben ist. Gerade der Baustein Zutrittskontrolle ist nur im Kontext eines übergeordneten Sicherheitssystems und im Zusammenhang mit anderen Bausteinen wie Zugriffs- oder Weitergabekontrolle geeignet, die Sicherheitsanforderungen der verschiedenen Beteiligten zu erfüllen, und er ist auch nur zusammen mit diesen wirklich wirksam.

Blick in die ComCard-Produktion



Herstellung einer Chipkarte

Vorgehensweise und Modelle

Das Sicherheitskonzept steht im engen Zusammenspiel mit den Systemen von Lieferanten, Partnern wie Auftraggebern und erfüllt dabei die Aufgabe, dass entlang dieser Kette kein Sicherheitsmangel zugelassen wird, der auch nur ansatzweise zur Kompromittierung einer Kundeninstallation beitragen könnte.

Schematisch folgt ComCard intern einem Modell, das sowohl in seinem logischen Aufbau wie auch der physischen Umsetzung als Schalenmodell umgesetzt ist. Das logische Modell folgt dem Prinzip, dass die Konzepte von der äußeren Schale einer unternehmensweiten Sicherheitspolitik bis zum Kern einer produktbezogenen Handlungsanweisung immer spezialisierter werden, dabei aber immer alle darüber liegenden Anforderungen zu erfüllen haben. Das physische Modell folgt der Tatsache, dass zum Beispiel der Zutritt zu den äußeren Bereichen geringeren Restriktionen unterliegt, zum Kern hin die Zutrittsberechtigungen indes immer mehr eingeschränkt werden. Der Wert der zu schützenden Objekte für das Unternehmen oder einen Angreifer steigt danach immer weiter an, je mehr sich ein potenzieller Eindringling dem Kern nähert.

Viele Einzelschritte zum gesamten Sicherheitssystem

Was heißt das in der Praxis? Ein sicherheitsrelevantes Produkt, sagen wir eine Prozessorchipkarte, wird im betrieblichen Durchlauf in mehreren Schritten produziert. Der Zusammenbau der Karte und elektrische Initialisierungsschritte des Chipmoduls erfolgen zwingend räumlich getrennt von der Personalisierung. Hier befinden sich höchst sensible Vorrichtungen, etwa Sicherheitsserver für geheime Informationen und Systeme mit Master-Schlüsseln.

Die an der Produktion beteiligten ComCard-Mitarbeiter besitzen differenzierte Zugangsberechtigungen zu den einzelnen Unternehmensbereichen. Die zur Produktion eingesetzte Software bedarf eines besonderen Schutzes; hier wird mit zur Außenwelt abgegrenzten Netzwerken gearbeitet. Der Zugriff auf sensible Daten erfolgt über definierte „Rollen", die die Rechte zum Zugriff auf Ressourcen des betreffenden Auftrags regeln.

Für jeden Mitarbeiter ist genau festgelegt, welche Räumlichkeiten er betreten darf

Dadurch lässt sich genau bestimmen, dass zum Beispiel nur ein Qualitätsbeauftragter des Unternehmens Statistiken für das Reporting an den Auftraggeber abrufen darf. Der Operator in der Produktionsumgebung kann wiederum nur mittels Leserechten aktuell eingestellte Aufträge zur Produktion bringen.

Im Gegensatz dazu sind zum Beispiel Besucher- und Besprechungsräume außen angesiedelt und unterliegen geringeren Restriktionen. Nach „draußen" müssen indes Schnittstellen zu Kunden und Firmen, die zum Beispiel ein externes Datenprozessing durchführen, aufgebaut werden, die den sicheren Datenaustausch gestatten. Hier wird nach dem Zonenprinzip gearbeitet, das durch diverse Vorkehrungen an den Zonenübergängen entsprechend hohe Hürden vorsieht.

Die organisatorischen Maßnahmen zeichnen sich durch exakte Handlungsanweisungen und eine konkrete Planung jeden Auftrags aus. Dabei gelten dann die internen Festlegungen des Unternehmens, es sind aber weiterhin IT-Sicherheitskonzepte und Eskalationspläne auftragsspezifisch mit dem Kunden festzulegen. Die Auditierbarkeit im Sinne der Zertifizierung, etwa für Kreditorganisationen, spielt beim Aufsetzen des Gesamtsystems für den Dienstleister eine wesentliche Rolle.

Unternehmen wie ComCard hoffen, auf diese Weise einen wesentlichen Grundstein dafür gelegt zu haben, auch in Zukunft das Vertrauen ihrer Kunden zu genießen, um erfolgreich Produkte für Banken sowie Ausweissysteme von Unternehmen anzubieten oder im eTicketing tätig zu sein. Die Arbeit mit persönlichen Daten von Kunden und Verbrauchern stellt eine stetige Verpflichtung zum verantwortungsvollen Umgang dar und ist damit zu Recht in diesen Tagen mehr den je im Fokus der Öffentlichkeit.

WWW.COMCARD.DE

Unser Autor Swen Hopfe ist Leiter Business Development bei der ComCard GmbH.