



Drei Audits auf

Foto: Ivan Dimitrov

einen Streich

Mehrere bestandene Audits, mehr Sicherheit und optimierte Prozesse: BORICA Ltd., die zentrale Instanz für Kredit- und Debitkarten in Bulgarien, zieht ein positives Fazit der Unterstützung durch SRC. SRC hat bei BORICA das MasterCard Logical Security Audit gemeinsam mit einem PCI DSS Security Audit und einem Audit der RINGS-Umgebung durchgeführt.

„Das war kein normales Audit. Wir haben darüber hinaus sehr viel Unterstützung von SRC bekommen und haben intensiv zusammengearbeitet.“

Christo Kostov
Head of Information Systems
BORICA Ltd.

||-- Kredit- und Debitkarten laufen in Bulgarien über die Systeme der BORICA. Die „Bank Organization for Payments Initiated by Cards“ (BORICA) ist eine Tochter der bulgarischen Nationalbank BNB sowie 22 weiterer Banken und die zentrale Instanz des Landes in Sachen kartengestütztem bargeldlosem Zahlungsverkehr. BORICA gibt unter anderem die führende gleichnamige bulgarische Debitkarte (vergleichbar mit der deutschen Girocard) heraus. BORICA ist in Bulgarien Third-Party-Processor von Visa International und MasterCard Worldwide sowie deren lokaler Partnerbanken. BORICA produziert und personalisiert obendrein bulgarische Debitkarten und Kreditkarten für beide großen Kartensysteme.

Anforderungen der Kartensysteme

-- Das Payment Card Industry Security Standards Council (PCI SSC), deren Mitglieder u.a.

MasterCard und Visa sind, haben mit dem PCI Data Security Standard (PCI DSS) Vorgaben formuliert, denen sich alle Unternehmen stellen müssen, die Kartendaten der internationalen Zahlungssysteme speichern, verarbeiten oder übermitteln. Zusätzlich verlangen Mastercard und Visa von Kartenherausgebern das jährliche Logical Security Audit sowie das Physical Security Audit. Logical Security bedeutet aus Sicht von MasterCard das Einhalten logischer Sicherheitsanforderungen im Prozess der Kartenpersonalisierung. Dabei werden z.B. Rollen- und Verantwortlichkeiten untersucht, die Sicherheitsplanungsanalysen, Verschlüsselungen unter die Lupe genommen, die Einhaltung des Vier-Augen-Prinzips überwacht und bauliche Umstände betrachtet: Wie und wo werden die Karten produziert, wie und wo werden sie vernichtet? Zur Logical Security kommen

die Anforderungen im Rahmen der Physical Security: Wie steht es beispielsweise um die Daten- und Netzwerksicherheit, wie sehen das User-Management und die Zugangskontrolle aus, wie steht es um die Software- und Hardware-Security und nicht zuletzt: Wie sind die baulichen Umstände, in denen die Kredit- und Debitkarten produziert und personalisiert werden?

Idee: Audits kombinieren

-- Die 1993 gegründete BORICA hatte bislang mit Hilfe großer international agierender Unternehmensberatungen die Audits und Anforderungen der Kreditwirtschaft absolviert. 2007 schrieb der bulgarische Kartenprozessor die Audits neu aus. SRC mit Sitz in Bonn gewann die internationale Ausschreibung gegen größere Mitbewerber. „SRC hat alle Anforderungen sehr genau erfüllt und bot die Audits außerdem durch die effiziente und integrierte Vorgehensweise zu den geringsten Kosten an“, begründet Christo Kostov, Head of Information Systems bei BORICA die Wahl. SRC habe an einer weiteren Stelle die Osteuropäer überzeugt: So hatte SRC vorgeschlagen, das MasterCard Logical Security Audit mit einem PCI DSS Security Audit und mit einem unabhängigen Audit von RINGS zu verbinden. RINGS steht für „Real Time Gross Settlement System“ und ist das zentrale Abrechnungssystem der bulgarischen Banken, das BORICA nach den Anforderungen der Regularien der BNB betreibt. Vorteil: Alle drei Prüfungen konnten zusammen und zu geringeren Kosten absolviert werden. SRC war zudem das einzige Unternehmen weltweit, das diese Audits aus einer Hand anbieten konnte. Zukünftig wird auch das MasterCard Physical Security Audit in die kombinierten Audits bei BORICA integriert. Christo Kostov: „Ein solches integriertes Angebot hat uns überzeugt.“ Heute lässt MasterCard nur noch Auditoren zu, die wie SRC fachlich in der Lage sind, beide Audits – Logical und Physical – durchzuführen. SRC ist aber derzeit das weltweit einzige Unternehmen, welches für MasterCard Logical und Physical Audits sowie PCI DSS Security Audits zugelassen ist.

Beratung on top

-- Bei der Arbeit in Sofia sollte sich bald herausstellen, dass BORICA mit SRC aus einem weiteren Grund die richtige Wahl getroffen hat: Während der Analysen zeigte sich, dass sich die Sicherheitsanforderungen in Sofia nicht einfach 1:1 umsetzen ließen. SRC unterstützte darum BORICA gleichzeitig mit Beratungsleistungen. Die Bonner konnten den Bulgaren dabei mit Erfahrung und Wissen aus einer Vielzahl von Projekten helfen. „Das war kein normales Audit“,

sagt Christo Kostov, „wir haben darüber hinaus sehr viel Unterstützung von SRC bekommen und intensiv zusammengearbeitet.“ So operiert BORICA beispielsweise mit einem Mainframe-System, bei dem sich eine Verschlüsselung von Kartennummern nicht klassischerweise umsetzen lässt. Durch das bei SRC vorhandene Mainframe-Know-how und mit technischen Finessen sowie eigens für BORICA entwickelten Sicherheitsmaßnahmen gelang es SRC und BORICA aber, die Anforderungen in Sachen Verschlüsselung zu erfüllen, berichtet Manuel Atug, Berater bei SRC. Experten von BORICA schauten sich mit Mitarbeitern der SRC in Bonn Firewall-Regelwerke und Sicherheitskonzepte an und nahmen wichtige Erkenntnisse mit auf den Rückflug nach Bulgarien. Das BORICA-Netzwerk wurde mit Hilfe von SRC so umstrukturiert, dass es heute höhere Sicherheitsanforderungen erfüllt. Christo Kostovs Eindruck: „SRC hat erfahrene Leute mit sehr viel Hintergrund-Wissen im Banking- und Payment-Sektor. Das finden wir sehr wertvoll.“

Tipps für Software-Tools

-- Weil SRC weiß, worauf die Auditoren abzielen, konnte man BORICA an mehreren Stellen helfen, den Anforderungen gerecht zu werden. Dazu gehörten auch Tipps für entsprechende Software-Tools aus dem neutralen Software-Listing von SRC. Die Bonner Experten unterstützten gleichzeitig praktisch: Weil die Zahlungssysteme alle Audit-Unterlagen in englischer Sprache brauchen, BORICA alle Dokumente aber nur in bulgarischer Sprache vorliegen hatte, half SRC bei der Übersetzung und vermittelte so zwischen Unternehmen und Auditoren. Und da BORICA einen Umzug plant, nahm SRC auch gleich die Baupläne für das neue Gebäude unter die Lupe und prüfte es entsprechend den Anforderungen der internationalen Zahlungssysteme. Derlei vorbereitet gingen die eigentlichen Audits ohne Beanstandung über die Bühne. Die Prüfer, berichtet Christo Kostov, seien beeindruckt gewesen, dass BORICA an einigen Stellen die Anforderungen übererfüllt habe. So rage beispielsweise das neue Passwortmanagement von BORICA deutlich über die Ansprüche des PCI-Standards hinaus. Für den bulgarischen Kartenprozessor und Karten-Emittenten haben die Audits mit Beratungsleistung einen guten Ausgang: Er erfüllt nun nicht nur schwarz auf weiß die internationalen Anforderungen, sondern er profitiert von einem Plus an Sicherheit, geringerem Risiko und von optimierten Prozessen. Dem IT-Chef Kostov gefällt darum die Bilanz. Er hat mit SRC einen längerfristigen Vertrag abgeschlossen und die Bonner Security-Berater für weitere Audits und Beratung engagiert. --||



Christo Kostov

BORICA Ltd.

117 Tzarigradsko Chaussee Blvd.

Sofia 1784

Bulgaria

Tel: +3592 9707 613

kostov.ch@borica.bg

<http://borica.bg/>



Detlef Kraus

Thilo W. Pannen

SRC Security Research & Consulting GmbH

Graurheindorfer Str. 149 a
D-53117 Bonn

Germany

Tel: +49 228 2806-0

sales@src-gmbh.de

<http://www.src-gmbh.de>