SEPA – Wird Missbrauch Tür und Tor geöffnet?

Kommentar von Johann Praschinger, Director Central Region ACI Worldwide

Die Banken ergreifen zunehmend Maßnahmen, um die SEPA-Vorgaben der Europäischen Kommission zu erfüllen. Es fehlt jedoch nach wie vor an eindeutigen Richtlinien und an einer zentralen Regulierungsstelle zur Überwachung der Umsetzung der SEPA-Richtlinien. Viele Banken werden daher die ab diesem Jahr geltenden ersten Fristen zur Umsetzung der SEPA-Vorgaben nicht einhalten. Eine der größten Herausforderungen ist dabei die Anpassung der IT-Infrastruktur an die neuen Bedingungen. Aufgrund des vereinfachten länderübergreifenden Geldflusses und Austauschs von Transaktionsdaten beginnen die Banken erst allmählich den Sicherheitsanforderungen, die SEPA mit sich bringt, Rechnung zu tragen. So haben viele Banken noch keine Strategien zur Missbrauchsbekämpfung implementiert, um sich und Ihre Kunden in der SEPA-Region zu schützen.

Johann Praschinger, Director Central Region von ACI Worldwide, zeigt die Risiken sowie Strategien auf, wie die Finanzindustrie in der SEPA-Region gegen drohenden Missbrauch vorgehen kann:

„Organisierte Finanzbetrüger sehen mit der Einführung von SEPA eine gute Gelegenheit, an Geld zu kommen. Mit SEPA wird der grenzüberschreitende Zahlungsverkehr noch einfacher und Missbrauch und Betrug wird regelrecht Tür und Tor geöffnet.

Nach der Einführung von EMV-Karten in Teilen Europas hat sich der Missbrauch auf Märkte verlagert, in denen noch keine EMV-Karten eingeführt waren und in den Bereich der Transaktionsabwicklung, die ohne Vorlage einer Karte möglich ist. Diese Erfahrung zeigt, dass die Wahrscheinlichkeit sehr groß ist, dass nach Einführung von SEPA ähnliche Entwicklungen und veränderte Betrugsmuster zu erwarten sind. Insbesondere Issuer und Acquirer, die EMV noch nicht im Sinne von SEPA eingeführt haben, werden vermehrt Betrugsversuchen ausgesetzt sein. Dies gilt gleichermaßen für Transaktionen ohne Karten, wie beispielsweise Lastschriften und Überweisungen innerhalb der SEPA-Region.

Die Gründung der FPEG (Fraud Prevention Expert Group), die für präventive Maßnahmen zur Bekämpfung von Betrug und Missbrauch auf länderübergreifender Ebene eingerichtet wurde, ist ein Schritt in die richtige Richtung. Dieser Organisation müssen jedoch auch Software-Anbieter und Processing-Dienstleister angehören, damit Missbrauch in der SEPA-Region, wie Phishing, Social Engineering, Geldwäsche, ID-Diebstahl und die Ausspähung von Kontonummern wirksam bekämpft werden kann.

Da es momentan noch keine verbindlichen Regelungen für die Sicherheit von SEPA-Transaktionen gibt, müssen die Banken sich des Ausmaßes des Problems bewusst werden und Strategien finden, die nicht nur die Vereinbarkeit mit diesen Vorgaben, sondern auch die Sicherheitsfrage im Auge haben. Um die Missbrauchs-Angriffe möglichst effizient einzugrenzen, braucht es einen zweistufigen Ansatz: Der Missbrauch muss direkt gestoppt werden, wo er entsteht, und die Transaktionen, bei denen dies nicht gelingt, müssen identifiziert werden. Dazu bieten sich Monitoring-Systeme an, die Transaktionen in Echtzeit überwachen, Log-On-Informationen im Internet nachverfolgen und selbständig die zuständigen Mitarbeiter alarmieren, sobald verdächtige IP-Adressen verwendet werden. Darüber hinaus müssen Banken in die Lage versetzt werden, verdächtiges Verhalten von Bankkunden zu erkennen. Schließlich sollten sie Two-Factor-Authentifizierungs-Techniken einsetzen, um die Sicherheit zusätzlich zu erhöhen.

Entscheidend ist weiter, dass Banken Informationen zu Missbrauch in Echtzeit mit anderen Finanzinstituten austauschen und ihre internen Silostrukturen aufgeben. Nur durch einen sowohl bankintern als auch –extern übergreifenden Ansatz kann Missbrauch in der SEPA-Region wirksam bekämpft werden.“

Für die Vereinbarung eines Hintergrundgesprächs mit ACI oder zur Anforderung ausführlichen Hintergrundmaterials wenden Sie sich bitte an Hotwire, Johannes Kaiser, 069-256693-35 oder johannes.kaiser@hotwirepr.com.