Kaspersky Fraud Prevention-Plattform: eine umfassende Lösung für die sichere Zahlungsabwicklung

Bankkunden von heute können die meisten ihrer Finanztransaktionen online durchführen. Laut einer weltweiten Umfrage unter Internetnutzern, die von B2B International und Kaspersky Lab durchgeführt wurde, nehmen 91 % der Befragten Online-Banking-Dienste in Anspruch[1]. Gleichzeitig waren jedoch 62 % der Befragten im Laufe des Jahres mindestens einmal Zielscheibe für einen Betrugsversuch oder andere Betrugsmaschen, d. h. sie liefen Gefahr, dass Geld von ihrem Konto gestohlen wurde.

Die Beliebtheit von E-Commerce zieht natürlich auch die Aufmerksamkeit von Cyberkriminellen auf sich. Laut CyberSource, einem Dienstleister für Zahlungsabwicklung und Risikomanagement, verloren E-Händler in den Vereinigen Staaten und Kanada 2012 rund 3,5 Milliarden USD aufgrund von Online-Betrug[2].

Die meisten Finanzinstitute versuchen, ihre Kunden durch Einführung der Mehrfaktorauthentifizierung und der Transaktionsbestätigung vor Cyberbedrohungen zu schützen. Darüber hinaus setzen sie für den Datenaustausch zwischen ihrem Online-Dienst und dem Benutzergerät Verschlüsselungstechnologien ein. Leider reichen diese Maßnahmen oftmals nicht aus, um den Gelddiebstahl zu vermeiden. Cyberkriminelle, die auf Angriffe im Finanzsektor spezialisiert sind, verfügen über eine breite Palette an Tools, die es ihnen ermöglichen, die Standardschutzbarrieren der Banken zu umgehen.

Kaspersky Lab erforscht und entwickelt seit vielen Jahren Technologien zum effektiven Schutz vor allen Arten von Cyberbedrohungen, einschließlich solcher, die auf den Finanzsektor abzielen. Auf diesem Wissen basiert die umfassende Kaspersky Fraud Prevention-Lösung von Kaspersky Lab, welche dem Online-Betrug den Kampf ansagt. Die Plattform bietet multifunktionalen Schutz bei allen Schritten einer Online-Transaktion und erfüllt rechtliche Vorschriften der Transaktionssicherheit.

Die Plattform enthält Clientprogramme, die für sichere Online-Zahlungen sorgen, und eine Serverlösung, die innerhalb der IT-Infrastruktur des Finanzinstituts zum Einsatz kommt. Außerdem verfügt sie über Kaspersky Fraud Prevention SDK. Dies ist ein spezielles Paket zur Entwicklung sicherer mobiler Apps auf Basis der Sicherheitstechnologien von Kaspersky Lab. Jede Transaktion durchläuft mehrere Authentifizierungsschritte. Dabei wird der Sicherheitsstatus des Benutzergeräts intensiv überwacht und kontrolliert. Sobald eine verdächtige Aktivität erkannt wird, werden Bankspezialisten vom System benachrichtigt.

Neben den Sicherheitstechnologien umfasst Kaspersky Fraud Prevention verschiedene Dienstleistungen wie Schulungen, Reporting zu Finanzbedrohungen usw.

[1] Security in a multi-device world: the customer's point of view (Sicherheit in der Welt vielfältiger Geräte: aus der Sicht des Kunden), Kaspersky Lab, August 2013

[2] CyberSource 2013-Bericht zum Online-Betrug

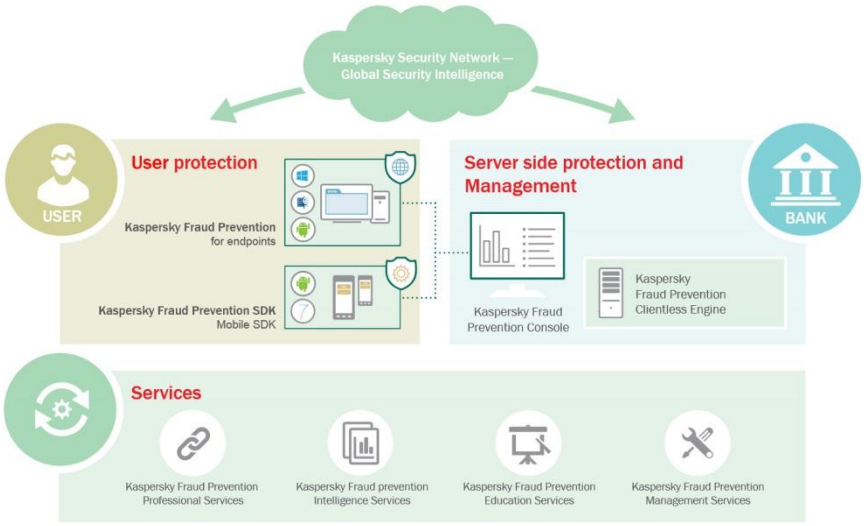

Abbildung 1: Die Kaspersky Fraud Prevention-Komponenten können einzeln oder als Komplettlösung eingesetzt werden.

Endpoint-Schutz

Clientgeräte sind meist die größten Schwachstellen bei jeder Online-Transaktion. Die Analyse der Daten, die Kaspersky Lab im Finanzsektor im Zeitraum von Cyberattacken aufgezeichnet hat, zeigt, dass in den meisten Fällen der Kunde Opfer von schädlichen Aktivitäten wird und nicht die Bank bzw. die Zahlungsinfrastruktur. Grundsätzlich sind Benutzer für den Schutz ihrer eigenen Geräte verantwortlich. Dennoch sind auf den Benutzergeräten nicht immer Sicherheitslösungen installiert, oder sie verwenden Antiviren-Produkte, die keinen dedizierten Schutz vor komplexen Finanzangriffen bieten. Kaspersky Fraud Prevention for Endpoints, das in der Kaspersky Fraud Prevention-Plattform integriert ist, umfasst spezielle Sicherheitstechnologien, die den Schutz bei der Nutzung von Online-Banking und elektronischen Zahlungssystemen sicherstellen.

Die Lösung unterstützt Windows, Mac, Android und iOS. Alle Programme bieten Datenschutz auf lokalen Geräten und verhindern das Abfangen von Daten bei der Übertragung zwischen einem Benutzergerät und einem Online-Finanzdienst.

Wenn ein Unternehmen (eine Bank oder ein Zahlungssystem) die Entwicklung eigener mobiler Apps für Android- oder iOS-Geräte in Erwägung zieht, kann dazu Kaspersky Fraud Prevention SDK eingesetzt werden. Dies ist ein Komponentenpaket zur leichteren Erstellung von Programmen basierend auf Sicherheitstechnologien von Kaspersky Lab.

Die Funktionsweise von Kaspersky Fraud Prevention for Endpoints ist am effektivsten, wenn die Daten über die Serverkomponenten der Plattform ausgetauscht werden. Das System verarbeitet statistische Daten der Kaspersky Fraud Prevention-Konsole und stellt sie Bankspezialisten zur Verfügung. Diese Konsole ermöglicht auch die Konfiguration von Kaspersky Fraud Prevention for Endpoints. Dies bedeutet: Wenn eine Bank einen neuen Online-Zahlungsdienst bereitstellt, erhalten die aktuell auf dem Benutzergerät installierten Programme automatisch alle Informationen, die benötigt werden, um sie vor Cyberangriffen zu schützen.

Erkennen betrügerischer Aktivitäten

In einigen Fällen können sich Kriminelle weiterhin Zugang zu Online-Konten verschaffen, indem sie Social-Engineering-Methoden anwenden, z. B. indem sie auf betrügerische Weise Daten über das Telefon abfangen. Doch selbst in diesen Fällen kann der Betreiber eines Finanzdienstes betrügerische Transaktionen über die Clientless Engine, eine Serverkomponente von Kaspersky Fraud Prevention, erkennen und blockieren.

Die Clientless Engine wird in die IT-Infrastruktur des Unternehmens integriert und sammelt Daten aus verschiedenen Quellen (abnormales Nutzerverhalten, Transaktionsinformationen). Die Daten werden an die Risiko-Engine gesendet, die zentrale Systemkomponente zur Durchführung eines Risiko-Assessments. Mit den folgenden Daten ermittelt die Risiko-Engine die Legitimität einer Transaktion:

- Berichte des Antiviren-Moduls des Servers, das Webseiten überprüft, auf die der Anwender während der Nutzung eines Online-Banking-Systems zugreift. Diese Komponente entdeckt schädlichen Code, der in eine scheinbar legitime Seite eingebettet wurde, um vertrauliche Daten zu stehlen.
- Mit der Analyse des Benutzerverhaltens während einer Online-Banking-Sitzung kann überprüft werden, ob Vorgänge vom Konto-Inhaber selbst und nicht von einem Dritten durchgeführt werden. Diese Funktion generiert ein Nutzerprofil.
- Daten vom Kaspersky Security Network[3], einschließlich Informationen über neue Cyberbedrohungen, sowie eine Datenbank, die speziell gemäß den Anforderungen von Finanzinstituten entwickelt wurde und Geräte mit einer niedrigen Reputation speichert. Ein Gerät kann aus vielen Gründen in der Datenbank gespeichert werden, z. B. wenn es mit Malware infiziert oder für verdächtige Zahlungen verwendet wurde.

Die Risiko-Engine empfängt die verarbeiteten Daten, und das System überprüft anhand eines flexiblen Regelpakets, ob ein Vorgang legitim ist. Gibt es einen Hinweis auf eine illegale Aktivität, informiert das System die Experten des Finanzinstituts über eine dafür vorgesehene Schnittstelle. Die Experten können dann entscheiden, ob die Transaktion genehmigt oder blockiert wird.

Die Clientless Engine kann den Schutz durch Informationen von Kaspersky Fraud Prevention for Endpoints erweitern. Die Serverkomponente funktioniert aber auch unabhängig von den anderen Plattformkomponenten. Die Clientless Engine ist nützlich, wenn ein Finanzinstitut oder Online-Shop Kunden schützen möchte, ohne Software auf Benutzergeräten zu installieren.

[3] Cloud-basierte Technologie des Kaspersky Security Network – Kaspersky Lab 2013

Intelligence und Education Services

Neben den von Kaspersky Fraud Prevention eingeführten Sicherheitstechnologien bietet Kaspersky Lab eine breite Palette an Schulungs- und Analysedienstleistungen:

- **Professional Services**: Bieten dem Finanzinstitut dedizierte Vorfallsuntersuchungen und Forensiken, die von einem Team aus Kaspersky-Experten durchgeführt werden.
- **Intelligence Services**: Regelmäßiges Reporting über Änderungen der Bedrohungslage im Finanzsektor.
- **Educational Services**: Experten von Kaspersky Lab bieten Schulungen für Mitarbeiter von Finanzinstituten an, welche das Thema „Diebstahl von Finanzdaten durch Malware“ behandeln.
- **Management Services**: Ein dedizierter Experte von Kaspersky Lab, der Sie bei der Lösung von Problemen im Zusammenhang mit Online-Banking-Bedrohungen unterstützt.

Vorteile von Kaspersky Fraud Prevention

Kaspersky Fraud Prevention bietet jedem Finanzinstitut, das Online-Transaktionen verarbeitet (Banken, Zahlungssysteme usw.) eine Vielzahl von Vorteilen:

- Fortschrittliche Technologien zum Schutz von Transaktionen auf Computern und mobilen Geräten
- Schnelle und einfache Integration in bestehende Lösungen zur Bekämpfung von Online-Betrug
- Echtzeitzugriff auf das umfassende Know-how von Kaspersky Lab zur Bekämpfung von Cyberbedrohungen

Der Schutz von Online-Finanzdiensten vor Cyberbedrohungen erfordert eine effektive Sicherheit auf allen Stufen des Transaktionsprozesses, von der Initiierung durch den Kunden bis zur Genehmigung durch das Finanzinstitut. Diese Anforderungen bilden die Grundlage der Kaspersky Fraud Prevention-Plattform: Die Lösung besteht aus einem mehrschichtigen Sicherheitssystem, dessen Komponenten nahtlos zusammenarbeiten, um für maximalen Schutz zu sorgen.

Somit ermöglicht die Kaspersky-Lösung Finanzinstituten, die Risiken, die durch Cyber-Angriffe entstehen und zu hohen Kosten und Rufschädigung führen, auf ein Minimum zu reduzieren.