KASPERSKY FRAUD PREVENTION – CLIENTLESS ENGINE

Mehr Sicherheit – besseres digitales Banking

Während Finanzinstitute sich bemühen, ihren Kunden ein möglichst intuitives und angenehmes Online-Banking-Erlebnis zu bieten, konzentrieren sich Cyberkriminelle auf die Entwicklung immer ausgeklügelterer Malware für den Online-Betrug.

Zu diesen leistungsstarken neuen Angriffsmethoden, deren Effektivität Sie vielleicht schon einmal am eigenen Leib erfahren mussten, gehören:

- **Infiltrieren von Webseiten** – Zusätzliche Felder, die in Ihre Anmeldeseite „injiziert" werden und vertrauliche Daten wie z. B. die CVC-Kartennummer erfassen, um sie für Kreditkartenbetrug zu nutzen.
- **Gefälschte Popup-Fenster (Phishing)** – Anzeigen eines eigenen, zusätzlichen Popup-Fensters, über das Betrüger weitere Daten, z. B. eine Mobilfunknummer, abfragen, um damit Authentifizierungscodes für die 2-Faktoren-Authentifizierung abzufangen.
- **Maipulation von Transaktionen** – Dem Kunden wird z. B. vorgegaukelt, er müsse einen irrtümlicherweise auf sein Konto überwiesenen Betrag zurückerstatten oder eine Testüberweisung ausführen, um die Bank bei der Einführung einer neuen Technologie zu unterstützen.

Voraussetzung für all diese Methoden ist die Infiltrierung Ihres Online-Banking-Systems durch das Einschleusen eines Banking-Trojaners. Das Einfallstor für diese Art von Malware ist in der Regel das schwächste Glied in Ihrem System – der Kunde. Die Angriffe starten mit der Infektion von Kundengeräten, von wo aus die Malware dann über eine Online-Verbindung in Ihr System eingeschleust wird.

Wie schützen Sie sich aber vor raffinierten Betrugsmaschen, die von den infizierten Geräten Ihrer Nutzer ausgehen, ohne das bequeme und einfache Online-Banking-Erlebnis zu gefährden, mit dem Ihre Kunden bisher so zufrieden waren?

Kaspersky Fraud Prevention Clientless Engine bekämpft Betrugsversuche durch:

Erkennung von Finanz-Malware:
Frühzeitige und aktive Suche und Identifizierung von Malware, die es darauf abgesehen hat, Ihre Webseiten über die Geräte Ihrer Kunden zu infizieren.

Erkennung von infizierten Computern oder Smartphones, die versuchen, über Online-Verbindungen zu Ihrer Website schädliche Aktivitäten auszulösen – ohne dabei nicht infizierte Kunden bzw. deren Online-Banking-Erlebnis zu beeinträchtigen.

Umfassendes Reporting:
Meldung von Vorfällen, damit Ihr Institut entsprechende Maßnahmen ergreifen kann, z. B.:

- Blockieren von Transaktionen
- Beenden der Benutzersitzung
- Problemlösung, damit sich der Vorfall nicht wiederholt

Endpoint Management:
Bereitstellen von Daten zum Vorfall über die Kaspersky Fraud Prevention-Konsole und Weitergabe der Daten an interne oder externe Systeme, um eine weiterführende Analyse oder Recherche zu ermöglichen

Feeds mit Bedrohungsinformationen:
Bereitstellen von Informationen an die Management-Teams Ihres Online-Banking-Systems, die sie für komplexe Sicherheitsentscheidungen benötigen

Während Sie den Überblick über jeden einzelnen potentiellen Sicherheitsvorfall behalten, verläuft der Vorgang für den Benutzer völlig reibungslos, es sei denn, sein Gerät wurde durch Banking-Malware kompromittiert. In diesem Fall können Sie Ihren Kunden bei einem sicheren Online-Banking unterstützen.

Das Ergebnis ist eine sicherere Online-Banking-Umgebung, in der Sie neue Kunden gewinnen und binden können, weil Sie die Möglichkeit haben, die Funktionalität Ihres digitalen Banking-Portals auszubauen, ohne dabei das Risiko unentdeckter Betrugsversuche zu erhöhen.

Kontaktieren Sie uns, um mehr zu erfahren: KFP@kaspersky.com
http://www.kaspersky.com/de/business-security/fraud-prevention

Informationsbroschüre zu Kaspersky Fraud Prevention Clientless Engine, August 2015 GL

KASPERSKY lab