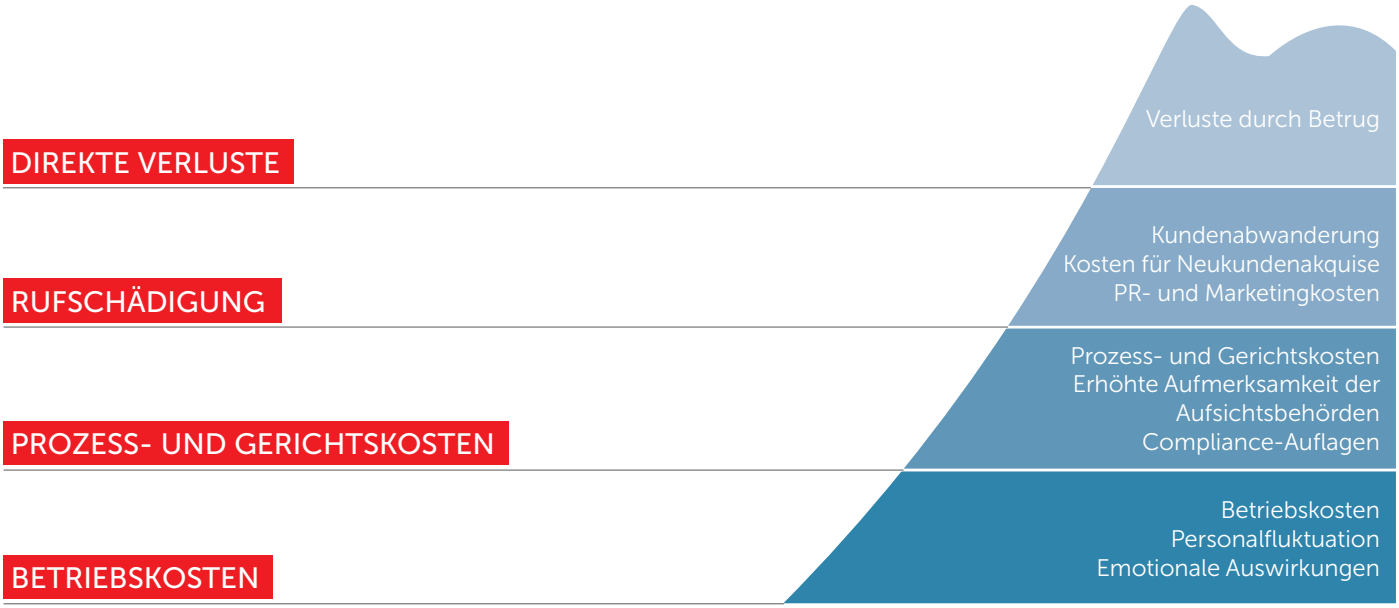
KASPERSKY FRAUD PREVENTION

Die Online-Finanzdienste Ihrer Bank sind gefährdet. Jede einzelne Sicherheitsverletzung kann eine Bank potentiell Zeit und und sehr viel kosten, wobei Erstattungen und Entschädigungen wirklich nur die Spitze des Eisbergs darstellen.

Die Spitze des Eisbergs: Gesamtkosten von Online-Betrug



Herkömmliche Sicherheitssysteme haben ihre Grenzen. Der Mensch bleibt auch weiterhin das schwächste Glied in der Sicherheitskette. Deshalb sind proaktive Schutz- und Entschärfungsmechanismen erforderlich, um zu verhindern, dass sich Nachlässigkeiten zu einer kostspieligen Krise auswachsen.

Die wahre Geschichte einer alltäglichen Cyberattacke

Stellen wir uns einen typischen Kunden vor – nennen wir ihn Herr Krüger. Während er wie gewohnt im Internet surft und in seinen Sozialen Netzwerken unterwegs ist, hat sich Herr Krüger ohne es zu merken, eine ausgeklügelte Malware eingefangen.

Als sich Herr Krüger bei seinem Online-Bankkonto bei Ihrer Bank anmeldet, setzt die Malware einen Banking-Trojaner ab, der zusätzliche Eingabefelder in die Anmeldeseite Ihres Webportals „injiziert". Für Herr Krüger macht die Seite jedoch weiterhin einen völlig normalen Eindruck, weshalb er ahnungslos seine Anmeldedaten inklusive Kennwort und Telefonnummer, die aus „Sicherheitsgründen" abgefragt werden, in die gefälschten Felder eingibt. Außerdem lädt er das neu bereitgestellte „Sicherheitszertifikat" (bei dem es sich natürlich ebenfalls um Malware handelt) herunter und installiert dieses auf seinem mobilen Gerät.

Dank Herr Krügers Kontozugangsdaten haben die Cyberkriminellen jetzt freie Hand und können sich an dem Geld auf seinem Online-Konto bedienen. Sie senden ihm per SMS Einmalkennwörter zur Bestätigung der Transaktionen, aber dank der Malware auf Herr Krügers Handy ist es für die Online-Betrüger ein leichtes, Ihre Nachrichten abzufangen.

Herr Krüger wollte eigentlich nur ein paar sichere Überweisungen tätigen – deshalb beantwortete er die „Sicherheitsfragen" der Betrüger und installierte die als „Sicherheitszertifikat" getarnte Malware auf seinem Smartphone. Bemerken wird er den Schwindel wahrscheinlich erst, wenn er das nächste Mal seinen Kontostand prüft. Und dann wird aus seinem Problem ganz schnell Ihr Problem.

Sie müssen Ihre Verteidigung stärken, um das Vertrauen Ihrer Kunden zu behalten, dass ihr Geld bei Ihnen sicher ist und ihre finanziellen Transaktionen vertraulich bleiben. Gleichzeitig müssen Sie Ihr Institut vor einer Vielzahl unterschiedlicher Attacken schützen und dazu ein ganzes Spektrum innovativer Technologien einsetzen.

Neben Sicherheit erwartet der Kunde jedoch gleichzeitig Online-Banking-Dienste, die sich einfach und bequem nutzen lassen. Der Grat zwischen einem benutzerfreundlichen Service und lückenloser Sicherheit ist sehr schmal: Unbedingte Sicherheit auf Kosten der Kundenzufriedenheit ist eigentlich kaum hinnehmbar.

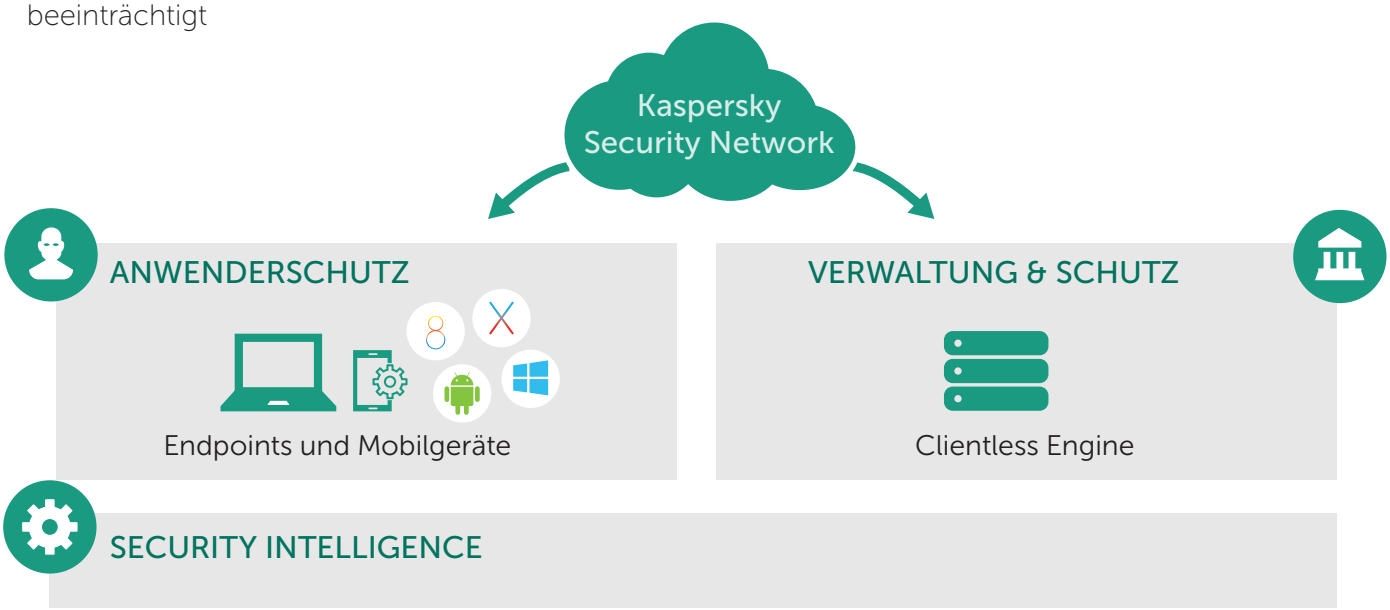
WIE SCHÜTZEN SIE IHRE KUNDEN UND SICH SELBST VOR ANGREIFERN, OHNE DIE SERVICEQUALITÄT IHRER BANK ZU BEEINTRÄCHTIGEN?

Die Schutztechnologien von Kaspersky Lab hätten in diesem Fall Folgendes geleistet:

- **Erkennung und Meldung der Malware,** welche die zusätzlichen Felder in Ihre Webseiten injiziert hat, und dass Herr Krüger in diesen Feldern Eingaben getätigt hat – **das gesamte Dilemma hätte also von vornherein verhindert werden können**
- **Identifizierung und Löschung des gefälschten „Sicherheitszertifikats",** bevor Herr Krüger es hätte installieren können
- **Speicherung aller von Ihrer Bank an Herrn Krüger gesendeten SMS-Nachrichten in einem** separaten, gesicherten Bereich auf Herr Krügers Handy, sodass ein Abfangen verhindert worden wäre
- **Effektiver Betrugsschutz, den Sie Herr Krüger hätten anbieten können, direkt auf den von ihm für das Banking genutzten Endgeräten**
- **Eine sichere und gleichzeitig einfache und bequeme Online-Banking-Erfahrung**

Kaspersky Fraud Prevention:

- Schützt Online- und mobile Banking-Systeme
- Verhindert frühzeitig alle gängigen Angriffsszenarien, die eine Bedrohung für Sie und Ihre Kunden darstellen könnten
- Sorgt für reibungslosen Schutz, der die Benutzerfreundlichkeit Ihrer Services nicht beeinträchtigt
- Nahtlose Integration in das Bankennetzwerk ohne Beeinträchtigung vorhandener Prozesse
- Lässt sich in Ihr Branding integrieren und individuell an Ihre Bedürfnisse anpassen



EINE LÖSUNG, DIE IHREM FINANZINSTITUT FOLGENDE VORTEILE BIETET:

- **Sichere und zufriedene Kunden** – Eine Engine ohne Client ermöglicht **benutzerfreundliche und proaktive Sicherheit für alle Kunden**, unabhängig davon, welches Gerät oder Plattform sie nutzen.
- **Kosteneinsparungen** – Weniger Betrugsvorfälle bedeuten **klare, quantifizierbare Einsparungen**, darunter **weniger direkte Verluste** durch Rückzahlungen an die Kunden, **entgangene Umsätze** durch Rufschädigung, **Prozess- und** Gerichtskosten, gesteigerte Aufmerksamkeit der Aufsichtsbehörden sowie **Betriebskosten**, etwa Zeit und Aufwand für die Untersuchung und Regulierung von Vorfällen.
- **Einen guten Ruf** – Vertrauen ist für jede Bank von entscheidender **Bedeutung, und Berichte über spektakuläre** Betrugsfälle können wertvolle Geschäftsbeziehungen zerstören, selbst wenn der Kunde von einer Sicherheitslücke nicht betroffen ist.
- **Ihre Marke** – Kaspersky Fraud Prevention lässt **sich individuell an die speziellen Bedürfnisse Ihres Unternehmens anpassen** und unterstützt und fördert so Ihre Marke.

MULTICHANNEL-BETRUGSSCHUTZ

Kaspersky Fraud Prevention deckt sowohl PC-basiertes als auch mobiles Online-Banking ab und erkennt und verhindert Betrugsversuche unabhängig davon, wie Ihre Kunden Bankgeschäfte betreiben oder welches Gerät sie dazu nutzen.

PROAKTIVER BETRUGSSCHUTZ

Kaspersky Fraud Prevention bietet **leistungsstarke, zusätzliche Schutzmechanismen** für Sie und Ihre Kunden, **die sich nicht negativ auf die Benutzererfahrung oder Ihre Geschäftsprozesse auswirken**.

Kaspersky Fraud Prevention sorgt nicht nur für die Abwehr von Angriffen – unsere Technologien hindern Betrüger aktiv daran, Kundendaten zu stehlen, **und ersticken Betrugsversuche so schon im Keim**.

BETRUGSSCHUTZ OHNE STÖRENDE NEBENWIRKUNGEN

Kaspersky Fraud Prevention unterstützt die bereits vorhandenen Sicherheitssysteme von Banken und erweitert sie um zusätzliche Erkennungsfunktionen. Auf diese Weise können Online-Betrugsversuche frühzeitig und ohne störende Nebenwirkungen erkannt werden, bevor sie zum Problem werden.

Die forensischen Funktionen von Kaspersky Fraud Prevention ermöglichen Ihren Spezialisten eine detailgetreue Aufklärung von Betrugsfällen und werden so zum leistungsstarken Verbündeten, wenn es darum geht, die Verantwortung Ihrer Bank zu klären und mögliche Kosten für Regulierung und Entschädigung zu reduzieren.

FUNKTIONSWEISE

Die Kaspersky Fraud Prevention-Plattform baut auf eigenen, **intern bei Kaspersky Lab entwickelten Technologien** auf, um Schutz vor der gesamten Bandbreite von Bedrohungen zu bieten, die es auf Banken und deren Kunden abgesehen haben:

Phishing – Bereits unmittelbar nach der Installation sorgt unser Cloud-Service, das Kaspersky Security Network, im Zusammenspiel mit hochmodernen heuristischen Verfahren dafür, dass aktuelle Phishing-Maschen erkannt und abgewehrt werden.

Malware, die es auf Kontozugangsdaten abgesehen hat – Cyberkriminelle entwickeln ausgeklügelte Programme, mit denen Attacken auf Internet-Banking-Kanäle gestartet, Konten übernommen oder Transaktionen umgeleitet werden sollen. Kaspersky Fraud Prevention sorgt dafür, dass infizierte Geräte keine Gelegenheit zum Zugriff auf das Online-System Ihrer Bank erhalten. Kunden, die bereits Betrugsversuchen zum Opfer gefallen sind, wird Kaspersky Fraud Prevention for Endpoints zur Korrektur angeboten.

Angriffe auf Online- und Mobile-Banking-Verbindungen – Kaspersky Fraud Prevention stellt sicher, dass die Verbindung des Benutzers zur Banking-Website geschützt ist, und verhindert so Man-in-the-Middle-Angriffe.

Browser-Infiltrierung und Web-Injektionen – Unsere Funktion „Sicherer Browser" wird bei jeder Online-Banking-Sitzung im Hintergrund geöffnet, verhindert Eingriffe in Browserprozesse und schützt Kundendaten auf diese Weise vor Malware, Screengrabs, Keylogging und Clipboard-Hacking.

Zusätzlicher Schutz für Mobile-Banking – **Datenschutztechnologien sorgen dafür, dass Zahlungsinformationen und die SMS-Kommunikation zwischen Benutzer und Bank nicht in die falschen Hände geraten.** Funktionen zur Risikoerkennung stellen sicher, dass mobile Geräte frei von Malware oder Schwachstellen bleiben, die finanzielle Transaktionen gefährden könnten.

WARUM KASPERSKY LAB?

Kaspersky Lab ist ein weltweit führender Anbieter von Cybersicherheitslösungen und kann auf fast zwei Jahrzehnte Erfahrung beim Kampf gegen die raffiniertesten Online-Bedrohungen zurückblicken. Über **400 Millionen Menschen auf der ganzen Welt** lassen sich von Kaspersky-Produkten schützen, **270.000 Unternehmen** vertrauen ihr Business dem Schutz durch unsere Technologien an.

Unsere einzigartige Expertise in den Bereichen Identifizierung und Schutz vor Cyberbedrohungen, darunter auch vor Angriffen auf Online-Finanzsysteme, ist ein elementarer Bestandteil unseres Unternehmens. Unsere Lösungen schneiden bei unabhängigen Tests beständig mit Bestnoten ab.

INTERNE FORSCHUNGSARBEIT – DIE GRUNDLAGE FÜR ZUVERLÄSSIGE SICHERHEIT

Kaspersky Lab ist eines der führenden Unternehmen im Bereich der Cyber-Sicherheitstechnologien, gerade weil wir ein besonderes Augenmerk auf interne Forschung und Entwicklung legen. Ein Drittel unserer 3.000 Mitarbeiter ist unmittelbar mit der Entwicklung der besten Sicherheitslösungen beschäftigt. Ca. 300 von ihnen konzentrieren sich auf die Erforschung neuer Bedrohungen für die Cybersicherheit und die Entwicklung innovativer, hochmoderner Schutzmethoden. Unsere Analysen haben ergeben, dass täglich **ca. 325.000 neue schädliche Dateien** hinzukommen, von denen viele speziell gegen Banken und Bezahlsysteme gerichtet sind. Zahlreiche Tests belegen, dass wir eines der führenden Unternehmen im Bereich der Erkennung und Abwehr von Cyberbedrohungen sind.

IM MITTELPUNKT STEHT DER MENSCH, NICHT NUR DIE TECHNOLOGIE

Wir schützen nicht nur Transaktionen, wir schützen die Menschen, die Ihrer Bank ihr Vertrauen schenken. Wir sind ebenso wie Sie an der Sicherheit und Zufriedenheit Ihrer Kunden interessiert. Dank einer Reihe unterschiedlicher Technologien zur Abdeckung der verschiedenen Angriffsvektoren bieten wir Ihren Kunden einen umfassenden und ganzheitlichen Schutz, egal wann und auf welche Weise sie Ihre finanziellen Dienstleistungen in Anspruch nehmen. Außerdem stellen wir sicher, dass das Kundenerlebnis bei der Nutzung Ihrer Services nicht durch unsere Schutzmechanismen beeinträchtigt wird.

UNMITTELBARER, ZUVERLÄSSIGER SCHUTZ

Im Kaspersky Security Network (KSN) – der komplexen, verteilten Infrastruktur von Kaspersky Lab – werden Daten über potenzielle Malware und auffällige Verhaltensmuster von den Geräten Millionen freiwillig teilnehmender Endbenutzer gesammelt und automatisch ausgewertet.

Dank der Fähigkeit von KSN, Daten über potenzielle Bedrohungen in Echtzeit auszuwerten, können die Endgeräte Ihrer Kunden viel schneller auf neu aufkommende Bedrohungen reagieren.

FLEXIBILITÄT

Kaspersky Fraud Prevention unterstützt Ihre Sicherheitsstrategie durch zusätzliche und lückenlose Schutzmechanismen (frühzeitige Erkennung und Prävention), die nahtlos in Ihre bereits vorhandenen Systeme integriert werden. Unsere Schutztechnologien verrichten Ihre Arbeit unauffällig im Hintergrund, ohne Sie oder Ihre Endbenutzer zu stören.

Die Kaspersky Fraud Prevention-Plattform besteht aus Kaspersky Fraud Prevention for Endpoint (für den Schutz von Windows-PCs und Macs) und dem Kaspersky Fraud Prevention SDK (für den Schutz von Endgeräten unter iOS, Android und Windows Phone). Zusammen ergeben diese Technologien einen leistungsstarken Schutz für Ihre Kunden, sparen Ihrer Bank Zeit und Geld und schützen den Ruf Ihres Unternehmens.

Kontaktieren Sie uns, um mehr zu erfahren: KFP@kaspersky.com

http://www.kaspersky.com/de/business-security/fraud-prevention

Whitepaper zur Kaspersky Fraud Prevention-Lösung, August 2015 GL