LexisNexis®
RISK SOLUTIONS

FALLSTUDIE

LexisNexis® Risk Solutions kann einen Beitrag leisten zur Einschränkung von Malware-Angriffen bei einem großen Finanzinstitut und reduziert somit Betrugsverluste

LexisNexis® ThreatMetrix® Digital Identity Intelligence deckt Hochrisiko-Ereignisse quasi in Echtzeit auf, ohne Einschränkungen für die Benutzererfahrung

AUF EINEN BLICK

UNTERNEHMEN

Ein großes Finanzunternehmen

VORAUSSETZUNGEN

- Verhinderung von gezielten Social-Engineering-Angriffen, basierend auf Remote Access Software, um sich Zugang zu offiziellen Benutzerkonten zu verschaffen.
- Einschränkung von Malware-Angriffen.
- Einschränkung von betrügerischen Ereignissen bei Login und Zahlungen.
- Reduzierung von Betrugsverlusten.

LÖSUNG

LexisNexis® Risk Solutions konnte ein umfassendes Behavioral-Profiling der End-to-End Online-Sitzung implementieren, einschließlich der Anlage von neuen Konten, Logindaten, Anpassung von Einzelheiten und Präferenzen sowie Konto-Navigation, Kreation neuer Begünstigter und Zahlungsprofilen, um Anomalien aufzudecken, die möglicherweise auf Malware, illegale Benutzer oder Remote Access Software hinweisen. Auf diese Weise konnte Betrug entschieden eingeschränkt werden, ohne dabei den Benutzerkomfort für die offiziellen Anwender einzuschränken.

FAZIT

- Innerhalb kürzester Zeit konnte gezielten Malware-Angriffen Einhalt gebieten werden, ohne falsche Positivergebnisse.
- Erkannte und blockierte Identitätsfälschungsversuche.
- Erkannte Man-in-the-Browser-Angriffe mit dem Versuch Anwender zu betrügen, um sie zur Preisgabe von personenbezogenen Daten zu bringen.
- Aufdeckung einer unrechtmäßigen Nutzung von Remote Access Software zum Hacken von Konten.
- Jeden Monat Einsparungen in Höhe von mehreren Millionen Dollar im Zusammenhang mit Betrugsverlusten.

FALLSTUDIE

Überblick

Dieses Finanzinstitut bietet eine umfassende Servicepalette, einschließlich Personal und Business Banking, Versicherungen, Corporate Finance sowie Private Banking. Im Rahmen der Philosophie der Bank stehen die Kundenwünsche im Mittelpunkt, weshalb sie einen umfassenden Premium-Service bietet. Der Schutz der Kunden vor Betrug sowie eine reibungslose Online-Erfahrung bilden das A und O der Geschäftstätigkeit.

Mit LexisNexis® Risk Solutions kann das Finanzunternehmen Folgendes tun:

- Vorgänge identifizieren, bei welchen Geräte eingesetzt werden, die versuchen, Fingerprinting-Technologien zu umgehen, indem die Browser-Version geändert wird oder indem Plug-ins im Browser installiert oder der Typ des Betriebssystems bzw. die Zeitzone angepasst werden.
- Erkennung der Anwesenheit von Malware, basierend auf der Analyse von Verhaltensmustern oder Anpassung von Webseiten, wobei betrügerische Vorgänge blockiert und verdächtige Events gemeldet werden.
- Erkennung von Remote Access Trojanern (RAT), die versuchen personenbezogene Informationen zu stehlen oder sich beim Anmeldeverfahren eines legalen Nutzers Informationen im Huckepackverfahren anzueignen.

Geschäftsproblem

Dieses Finanzinstitut war – wie zahlreiche andere auch – vermehrt Opfer von Social-Engineering-Angriffen, in deren Rahmen von den Benutzern häufig unwissentlich Remote Access Software oder Malware installiert wurde. Teilweise gelang es bei diesen Angriffen sogar, starke Zwei-Faktor-Authentifizierungsbarrieren zu umgehen, weil beispielsweise die Daten von Login-Sitzungen mit einer umfassenden Authentifizierung im sogenannten Rucksackverfahren angeeignet wurden.

Bei einem Zugriff der Anwender auf die Website, einer Anmeldung in ihrem Bankkonto, Zahlungen, Passwortänderungen usw. versuchte diese Malware Klicks zu überwachen und Felder mit personenbezogenen Daten zu hacken, wie beispielsweise Kundenname, Kontonummer, Passwörter und andere vertrauliche Daten.

Das Finanzinstitut brauchte eine robuste Betrugsbekämpfungslösung, die in der Lage war, aktuelle Vorgänge zu analysieren und mit Verhalten in der Vergangenheit zu vergleichen, um Anomalien in Echtzeit genau identifizieren zu können. Anschließend kann das anomale Verhalten geprüft oder direkt blockiert werden, abhängig vom jeweiligen Risikoniveau.

FALLSTUDIE

Das Finanzinstitut brauchte eine robuste Betrugsbekämpfungslösung, die in der Lage war, aktuelle Vorgänge zu analysieren und mit Verhalten in der Vergangenheit zu vergleichen, um anomales Verhalten in Echtzeit genau identifizieren zu können.

Die Macht der globalen Shared Intelligence bei der Erkennung von Hochrisikoereignissen nutzen Ereignisse quasi in Echtzeit

Die beste Möglichkeit beim Umgang mit komplexen, organisierten Cyberverbrechen ist der Einsatz der Macht eines globalen, gemeinsam genutzten Netzwerks. Das LexisNexis® Digital Identity Network® sammelt und verarbeitet globale Shared Intelligence von Millionen täglichen Verbraucherinteraktionen, wie Anmeldungen, Zahlungen und neue Kontoeröffnungen. Durch den Einsatz der Produktfunktionen von LexisNexis® ThreatMetrix® und unter Nutzung von Informationen aus dem Digital Identity Network® kann das Unternehmen für jeden Anwender eine unverkennbare digitale Identität anlegen, indem die unzähligen Verbindungen zwischen Geräten, Standorten und anonymisierten individuellen Informationen analysiert werden. Verhalten, das von dieser vertrauenswürdigen digitalen Identität abweicht, kann quasi in Echtzeit genau erkannt werden, wodurch das Finanzinstitut auf potenziellen Betrug hingewiesen wird. Verdächtiges Verhalten kann erkannt und für die Überprüfung, Step-up-Authentifizierung oder Ablehnung gekennzeichnet werden, bevor eine Transaktion verarbeitet wird, sodass vertrauenswürdige Benutzer weniger Stress haben.

Dank des ThreatMetrix®-Produkts konnte Folgendes erzielt werden:

- Erkennung von vertrauenswürdigem Verhalten und Zuordnung für die einzelnen Anwender (Geräte, IP-Adressen, Standorte, Sitzungs- und Zahlungsverhalten).
- Identifizierung von ungewohnten Verhaltensänderungen zur Verhinderung von Zahlungsbetrug, einschließlich der Identifizierung von Remote Access Software sowie Malware-Signaturen.
- Identifizierung der Anwesenheit von anhaltenden Betrugsnetzwerken durch die Schaffung von Verbindungen aus bekannten Mule Accounts oder basierend auf an anderen Stellen des LexisNexis® Risk Solutions Network aufgedecktem betrügerischem Verhalten.
- Identifizierung von ungewöhnlichem Verhalten im Zusammenhang mit Insiderbetrug.

FALLSTUDIE

Zentrale Funktionen der LexisNexis® ThreatMetrix®-Lösung

- **Dank Fingerprinting-Technologien** für Seiten können alle Änderungen einer Seite erkannt werden, wie die Injektion von HTML- oder JavaScript-Komponenten durch Malware in Echtzeit, sodass Online-Transaktionen geschützt werden.
- **Dank Malware-Schutz** können Unternehmen selbst das Risiko der ausgeklügelsten Malware einschränken und somit Betrug reduzieren. Hierzu zählen auch Man-In-The-Browser (MITB), Remote Access Trojaner (RAT), schnelle/Hochfrequenz Botnet-Angriffe sowie langsam durchgeführte Angriffe, die ein legitimes Kundenverhalten nachahmen, Ransomware, Key Logging-Versuche usw.
- **Die Erkennung von Malware und die Einstufung von Anwendungen** im mobilen Software Development Kit (SDK) zur Bewertung aller auf Android-Geräten installierten Anwendungen sowie Prüfung basierend auf einer branchenführenden Signatur-Datenbank mit über 15 Millionen mobilen Apps. Validierung von bekannten, vertrauenswürdigen Anwendungen und Meldung von Anwendungen mit Malware oder einem schlechten Ruf quasi in Echtzeit.
- **Honeypot-Technologie** zum Setzen von Fallen zur Aufdeckung von unzulässigen Website-Modifikationen im Browser. Mit der Honeypot-Falle wird die Malware getäuscht: Es sieht so aus als würde ein Anwender sich auf eine der normalerweise von Malware anvisierten Website mit hochwertigen Informationen begeben. Die Malware versucht daraufhin einen Angriff, indem zusätzliche Webinhalte injiziert werden, wie ergänzende Formularelemente oder Popup-Fenster mit der Frage nach personenbezogenen Informationen. Diese Änderungen werden von unserem Honeypot in Echtzeit erkannt.
- **Die Funktionen von LexisNexis® Risk Solutions** können zusätzlich verstärkt werden, indem über einen Integration Hub weitere externe Threat Intelligence Feeds integriert werden. Der Integrations-Hub ermöglicht Institutionen, wichtige Datenquellen von Drittanbietern und maßgeschneiderte Services zu integrieren, um zusätzliche Services für Authentifizierungen und Identitätsüberprüfungen von hochriskanten Transaktionen anzubieten.

LexisNexis® RISK SOLUTIONS

Wenn Sie weitere Informationen möchten, rufen Sie 866.528.0780 an oder besuchen Sie risk.lexisnexis.com/FIM-EN

About LexisNexis Risk Solutions

LexisNexis Risk Solutions harnesses the power of data and advanced analytics to provide insights that help businesses and governmental entities reduce risk and improve decisions to benefit people around the globe. We provide data and technology solutions for a wide range of industries including insurance, financial services, healthcare and government. Headquartered in metro Atlanta, Georgia, we have offices throughout the world and are part of RELX Group (LSE: REL/NYSE: RELX), a global provider of information and analytics for professional and business customers across industries. RELX is a FTSE 100 company and is based in London. For more information, please visit www.risk.lexisnexis.com, and www.relx.com

About ThreatMetrix

ThreatMetrix®, A LexisNexis® Risk Solutions Company, empowers the global economy to grow profitably and securely without compromise. With deep insight into 1.4 billion tokenized digital identities, LexID® Digital delivers the intelligence behind 110 million daily authentication and trust decisions, to differentiate legitimate customers from fraudsters in near real-time.

LexisNexis, LexID, and the Knowledge Burst logo are registered trademarks of RELX. ThreatMetrix and Digital Identity Network are registered trademarks of ThreatMetrix, Inc. Copyright © 2019 LexisNexis Risk Solutions.

Learn more at risk.lexisnexis.com/FIM-EN. NXR14090-00-0919-EN-US