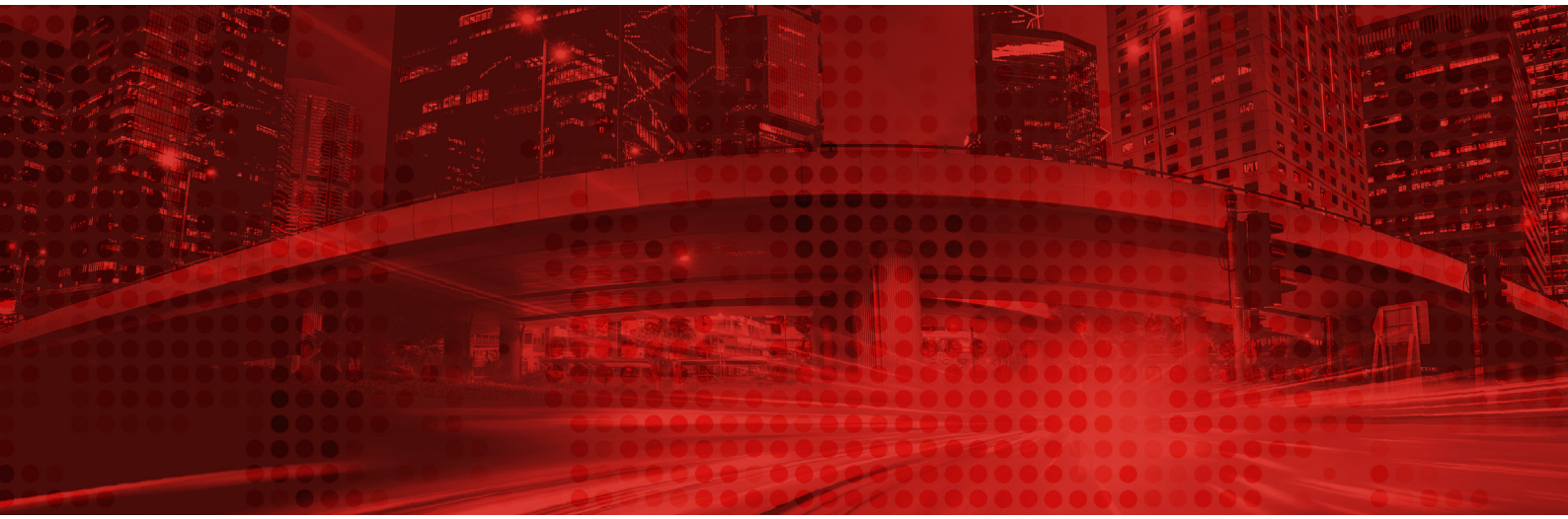
RSA® FRAUDACTION™ 360



Einführung

Der Online-Channel hat noch nie ein so innovatives, global integriertes kriminelles Netzwerk erlebt wie heute. Kriminelle verfügen mittlerweile über fortschrittlichste Technologien und betreiben eine raffinierte Schattenwirtschaft:

- Das Phishing nimmt weiter zu.
- Trojaner sind ausgefeilter und leichter zu bekommen.
- Nicht autorisierte mobile Apps infiltrieren öffentliche App Stores.
- Social Media sind voll mit gefälschten Firmenseiten.

Bisherige Erfolge von RSA® FraudAction™:

- Abwehr von über 2 Millionen Cyberangriffen
- Identifizierung von über 1 Milliarde Cyberangriffen weltweit
- Wiederherstellung von mehreren Hundert Millionen kompromittierter Zugangsdaten

Auf einen Blick

Durchgängiger Schutz vor Phishing, Trojanern, nicht autorisierten mobilen Apps und Social Media-Bedrohungen – von der Erkennung bis zur Sperrung

Berichte und Feeds zu den neuesten Onlinebedrohungen, einschließlich neuer Betrugstrends

Zugriff auf detaillierte Angriffsberichte über das RSA FraudAction-Dashboard – das Reporting-Onlineportal

Ein allumfassender Schutz vor diesen verschiedenen Arten von Angriffen ist wichtig, da sie immer stärker ineinandergreifen. So verfügen Trojaner nicht selten auch über eine mobile Anwendungskomponente. Social Media sind zu einer neuen Oase für gefälschte Firmenwebsites geworden, die von Cyberkriminellen entwickelt wurden, um Verbraucher zu täuschen.

Wenn es um einen Komplettschutz vor Betrug geht, so stehen die Unternehmen vor der Herausforderung, mehrere Anbieter zu managen, d. h. mehrere Servicekennzahlen, Budgetanforderungen und Geschäftsbeziehungen, da Services für verschiedene Bedrohungsvektoren von verschiedenen Anbietern angeboten werden – oder Sie müssen selektiv vorgehen und einen Bedrohungsvektor gegenüber anderen vorziehen und gehen damit das Risiko ein, für bestimmte Arten von Angriffen anfällig zu sein.

RSA FraudAction 360

Um sich gegen die komplexen Angriffsmuster von heute zu wehren, kombiniert RSA FraudAction 360 alle Bedrohungsvektoren in einem umfassenden Service für das externe Bedrohungsmanagement, um einen vollständigen Schutz vor Phishing, Trojaner-Angriffen, nicht autorisierten Apps und Social Media-Bedrohungen zu implementieren. Darüber hinaus können Kunden mit Intelligence-Berichten, die detaillierte Einblicke in die Cyberkriminalität gewähren, ein tieferes Verständnis bezüglich neu aufkommender Bedrohungen entwickeln.

Minimierung externer Bedrohungen

Mit einem allumfassenden Service haben Unternehmen folgende Vorteile:

- Bereitstellung weniger interner Ressourcen für das Management externer Bedrohungen
- Rundumschutz vor Betrug, bei dem kein Bedrohungsvektor ausgelassen wird
- Management von nur einem Anbieterbudget für eine Rund-um-die-Uhr-Betrugsbekämpfung

Der Service von RSA FraudAction 360 für das externe Bedrohungsmanagement umfasst die folgenden Komponenten:

- Schutz vor Phishing
- Schutz vor Trojanern
- Schutz vor nicht autorisierten mobilen Apps
- Schutz vor Bedrohungen durch Social Media
- Ausgewählte Feeds und Berichte von RSA FraudAction mit intelligenten Daten

Schutz vor Phishing

RSA FraudAction erkennt und minimiert Phishing-Angriffe. Der Service hilft Unternehmen dabei, unmittelbar auf einen Angriff zu reagieren und danach detaillierte Untersuchungen anzustellen.

Überwachung und Früherkennung

RSA wendet mehrere Strategien zur Früherkennung an, z. B. die Überwachung neu registrierter Domains und Weblogs von Kunden. Die Erkennungsressourcen von RSA FraudAction ermöglichen es unseren Analysten, Milliarden von URLs pro Tag zu scannen, z. B. missbrauchte Postfächer von Kunden, und eine automatisierte heuristische und manuelle Qualifizierung verdächtiger URLs durchzuführen.

Warnmeldungen und Reporting in Echtzeit

Wenn eine verdächtige URL als Bedrohung bestätigt wurde, werden die Kunden umgehend benachrichtigt und können die neuesten Bedrohungsinformationen und den Status über das RSA FraudAction-Dashboard in Echtzeit überwachen. Das Reporting-Onlineportal bietet außerdem Sperrzeitpläne sowie branchenspezifische und geografische Trends.

Exklusives Netzwerk zur Sperrung von Websites

RSA ist mit seinem Sperr-Feed für mehr als 96 % des weltweiten Webverkehrs zur ersten Verteidigungslinie geworden, sowohl für Nutzer aller gängigen Internetbrowser, einschließlich mobiler Browser, als auch für Kunden führender Datensicherheitsanbieter und ISPs. Sobald Angriffe erkannt werden, werden nahezu in Echtzeit Feeds über Phishing-Websites an diese Unternehmen gesendet, sodass sie diese Websites innerhalb von Minuten nach Erkennung blockieren können.

Abschaltung von Phishing-Websites

RSA nutzt seine langjährigen Beziehungen zu mehr als 16.000 verschiedenen Hosting-Stellen sowie seine Mehrsprachigkeit, um eine schnelle, globale Abschaltung betrügerischer Websites zu ermöglichen. Bis dato konnte RSA die Abschaltung von mehr als einer Million betrügerischer Websites bewirken, die in mehr als 187 Ländern gehostet wurden.

Schutz vor Trojanern

RSA FraudAction erkennt und verringert auch die Schäden, die durch Trojaner-Angriffe verursacht werden. Der Service identifiziert Malware-Bedrohungen, reagiert sofort auf einen Angriff und minimiert das davon ausgehende Risiko, indem der Endnutzerzugriff auf die Onlineressourcen des Angriffs blockiert wird.

Identifizierung und Analyse

RSA FraudAction hat ein Netzwerk aus Partnern aufgebaut, um eine möglichst hohe Erkennungsgenauigkeit zu erreichen. Dieses Netzwerk umfasst Unternehmen aus verschiedenen Technologiebereichen, darunter Anbieter von Virenschutzsoftware für Privatanwender, Geheimdienststellen und Internet-Gateways.

Bedrohungsberichte von RSA FraudAction

RSA FraudAction 360-Kunden erhalten Bedrohungsberichte mit aufschlussreichen Informationen, z. B. zu Betrugstrends, neuen Betrugsmethoden oder neuen Tools und Services für Cyberkriminelle, die im Untergrund angeboten werden.

Die Bedrohungsberichte von RSA FraudAction benachrichtigen Kunden über neue Sicherheitslücken, die entdeckt wurden oder von Betrügern aktuell genutzt werden, sowie über Auszahlungs- oder andere Methoden, die Betrüger bei ihren Angriffsversuchen auf Unternehmen anwenden.

Wenn ein RSA FraudAction-Partner Malware erkennt, werden die Informationen über den Trojaner zur Untersuchung an das RSA Anti-Fraud Command Center (AFCC) gesendet. Erfahrene Analysten führen statische und dynamische Analysen durch, um die Auslöser, Kommunikationspunkte und andere Daten sowie den Modus Operandi des Trojaners in einem infizierten System zu erforschen. Sofern möglich werden auch die jeweiligen „Haltepunkte" des Trojaners überwacht, um zu versuchen, die kompromittierten Zugangsdaten wiederherzustellen.

Abschaltungen

RSA schaltet im Kundenauftrag betrügerische Websites ab, die mit den Infektionspunkten der einzelnen Angriffe verbunden sind. Nachdem die betrügerischen Websites aufgespürt und analysiert wurden, initiiert das RSA AFCC die Schließung der Website mit einem Unterlassungsverfahren, indem es mit ISPs, Webhosting-Einrichtungen und Domainregistrierungsstellen interagiert.

Schutz vor nicht autorisierten mobilen Apps

RSA FraudAction hilft Unternehmen dabei, Betrugsverluste zu reduzieren, indem der Service gegen bösartige oder nicht autorisierte mobile Apps vorgeht. Der Service überwacht alle größeren App Stores, spürt Apps auf, die es auf die Kundendatenbanken von Unternehmen abgesehen haben, und sperrt die nicht autorisierten Apps. Dadurch werden Bedrohungen für die Reputation der Unternehmen sowie finanzielle Verluste aufgrund von Betrügereien durch diese Apps reduziert.

Überwachung und Erkennung

Der Service bietet kontinuierliche Einblicke in die App Stores und stellt für die Unternehmen eine proaktive Onlineabwehr zur Verfügung. Die kontinuierliche Überwachung der App Stores hilft den Unternehmen dabei, potenziellen Bedrohungen immer einen Schritt voraus zu sein und diese schon zu kennen, wenn eine autorisierte App in Erscheinung tritt.

Sperrung nicht autorisierter Apps

Nach der Erkennung der App und der Genehmigung deren Sperrung leitet RSA die Entfernung der nicht autorisierten App ein. Der Service sorgt dafür, dass die Kunden die vollständige Kontrolle über Apps behalten, die ihr Unternehmens repräsentieren, sodass nur die von ihnen bereitgestellten bzw. autorisierten Apps am Markt verfügbar sind. Durch den Service wird außerdem sichergestellt, dass Kunden und Hunderte Millionen Nutzer mobiler Apps nicht auf Phishing, Malware und sonstige nicht autorisierte Apps zugreifen, und zwar noch bevor die Apps veröffentlicht werden bzw. in den App Stores Popularität erlangen.

Kundenfeedback

> *Durch die Implementierung von RSA FraudAction waren wir schneller in der Lage, Phishing-Angriffe zu neutralisieren, und zwar innerhalb weniger Stunden statt Wochen. Darüber hinaus haben wir Betrugsverluste in Höhe von mehreren Millionen tschechischen Kronen verhindert, was gut für uns und – was noch wichtiger ist – unsere Kunden ist.*

Großes europäisches Finanzinstitut

Schutz vor Bedrohungen durch Social Media

Social Media haben sich als wichtiger Kommunikationskanal etabliert, um Ihre Marke und die dazugehörigen Serviceangebote mit Ihren Kunden zu verbinden. Da über Social Media neue Bedrohungsvektoren hinzugekommen sind, missbrauchen Cyberkriminelle nun vermehrt Social Media-Seiten, um Betrug zu begehen oder betrügerische Transaktionen zu starten. Für die Unternehmen ist es eine große Herausforderung, die Risiken über alle digitale Channels, einschließlich Social Media, kontinuierlich zu überwachen, denn mit den intern zur Verfügung stehenden manuellen Ressourcen kann man den Anforderungen des Risikomanagements nur schwer gerecht werden.

RSA FraudAction bietet transparente Einblicke in Social Media-Seiten und hilft den Unternehmen so dabei, zwischen autorisierten Firmenseiten und potenziell gefährlichen Seiten zu unterscheiden. Durch die Social Media-Überwachung identifiziert RSA FraudAction Seiten, die direkt mit betrügerischen Aktivitäten verknüpft sind, die ggf. auf Ihr Unternehmen abzielen oder versuchen, Ihre Kunden irrezuführen, indem sie sich als Ihr Unternehmen und/oder als Tochterfirmen ausgeben. Mithilfe von RSA FraudAction können Unternehmen Bedrohungen über Social Media schnell abwehren, bevor es zu schweren und langfristigen Schäden kommt.

RSA FraudAction Cyber Intelligence

RSA FraudAction Cyber Intelligence bietet Einblicke in die Trends der Cyberkriminalität sowie tiefergehende Untersuchungen globaler Betrugsmethoden und -aktivitäten.

Kostenlose Feeds und Berichte des RSA FraudAction Cyber Intelligence-Service der Stufe 1 sind in RSA FraudAction 360 ohne zusätzliche Kosten enthalten. Diese Berichte und Datenfeeds zu Bedrohungen lassen sich problemlos in andere Backend-Systeme integrieren.

So werden die intelligenten Informationen von RSA FraudAction 360 bereitgestellt:

- **IP-Feed:** Tägliche Liste mit hochriskanten IPs, z. B. Proxies/Socks und RDPs
- **E-Mail-Feed:** Tägliche Liste der kompromittierten E-Mail-Adressen von Mitarbeitern und Spam-Mails
- **Feed zu Mule Accounts:** Liste mit Mule Accounts, die von den RSA-Analysten wiederhergestellt wurden
- **Feed zu Lieferadressen:** Liste mit physischen Postanschriften, an denen die mit gestohlenen Karten erworbenen Produkte entgegengenommen werden
- **Kreditkarten-Feed:** Liste mit kompromittierten Kreditkartendaten, die „im Untergrund“ verfolgt werden
- **Vierteljährlicher Newsletter:** Globale Statistiken zu Phishing und Trojanern sowie eine Übersicht der gemeldeten Trends aus dem letzten Quartal
- **Bedrohungsberichte:** Berichte über neue Angriffsmethoden und Trends im Bereich der Cyberkriminalität

Die RSA Fraud & Risk Intelligence Suite

Die RSA® Fraud & Risk Intelligence Suite versetzt Unternehmen in die Lage, Risiken über privatanwenderorientierte digitale Channels im Griff zu behalten, sodass sie ihre Umsätze maximieren und Betrugsverluste minimieren können. Die Suite gehört zum RSA-Portfolio unternehmensgesteuerter Sicherheitslösungen, die einen einheitlichen Ansatz für das Management digitaler Risiken bieten, der auf integrierter Sichtbarkeit, automatisierten Einblicken und koordinierten Maßnahmen basiert. RSA schützt Millionen von Nutzern auf der ganzen Welt und trägt dazu bei, dass mehr als 90 % der Fortune 500-Unternehmen erfolgreich sind und sich kontinuierlich an tiefgreifende Änderungen anpassen können. Weitere Informationen finden Sie unter rsa.com/de-de.

10/19 Lösungsübersicht H16793 W294028.