E-Mail-Link-Isolierung

Isolieren Sie E-Mail-Links, um die Angriffsfläche zu verringern und die Abläufe zu vereinfachen

Verringern Sie das Phishing-Risiko, indem Sie Schutzmaßnahmen und Kontrollen zur Browserisolierung anwenden

Herausforderung: Raffiniertes Phishing über mehrere Kanäle

Phishing über mehrere Kanäle erstreckt sich über E-Mail und Internet und kann so Filterregeln geschickt umgehen. Zu den gängigen Arten gehören:

- **Deferred Phishing**: Ein ursprünglich harmloser Link in einer E-Mail wird nach der Zustellung mit einem bösartigen Ziel versehen.
- **Cloud-Service-Phishing:** Gefährliche HTTPS-Links, die gängigen Cloud-Diensten sehr ähnlich sind (z. B. Google Drive, Box)

Um Bedrohungen wie diese abzuwehren, muss ein moderner E-Mail-Schutz in der Lage sein, alle Links nach dem Zero-Trust-Prinzip („Niemals vertrauen, immer verifizieren“) zu prüfen.

Lösung: Isolierung von E-Mail-Links

Durch die Integration von Remote-Browserisolierung (RBI) mit Cloud E-Mail-Sicherheit (CES) wird der Phishing-Schutz noch weiter verbessert. Kunden von Cloudflare Area 1 können Cloudflare Browserisolierung aktivieren, um diese über mehrere Kanäle agierenden Bedrohungen zu neutralisieren.

Administratoren können die Interaktionen von Nutzern auf isolierten Webseiten kontrollieren (z. B. Tastatureingaben und Dateiuploads einschränken), um Phishing-Attacken wie das Abgreifen von Zugangsdaten oder den Diebstahl vertraulicher Daten zu verhindern.

Außerdem neutralisiert das Öffnen von E-Mail-Links in einem isolierten Browser Malware, da der gesamte Code in der Cloud ausgeführt wird, fernab von lokalen Geräten.

Was Analysten sagen:

„E-Mail-basierte URLs, die extern aufgelöst werden, werden häufig für Phishing-Attacken auf Mitarbeiter verwendet. Isoliert man diese, kann dies die Anzahl erfolgreicher Phishing-Angriffe reduzieren.“

„Die meisten Angriffe erfolgen über das öffentliche Internet, entweder über das Surfen im Internet oder über per E-Mail verschickte Links, die den Nutzer dazu verleiten, bösartige Websites zu besuchen. Das einfache Entfernen (oder besser noch das Isolieren) des Browsers vom Desktop des Endbenutzers verbessert die Sicherheitslage des Unternehmens erheblich, einschließlich des Schutzes vor Ransomware-Angriffen.“

„Evaluieren und testen Sie eine Lösung zur Browserisolierung für bestimmte Nutzer mit hohem Risiko (z. B. Finanzteams) oder Anwendungsfälle (z. B. das Rendern von E-Mail-basierten URLs), insbesondere wenn Ihr Unternehmen risikoavers ist.“[1]

Gartner

Weitere Informationen

Geschäftliche Vorteile der Integration von CES & RBI

Phishing-Schutz verstärken

Die E-Mail-Isolierung verhindert nicht nur, dass schädlicher Code in einem Phishing-Link lokal ausgeführt wird, sondern wendet auch Datenschutzkontrollen an, um zu verhindern, dass sensible Informationen in die falschen Hände geraten.

Produktivität von IT- und Sicherheitsteams steigern

Aktivieren Sie die E-Mail-Isolierung für jede Website mit ein paar Klicks.

IT- und Sicherheitsteams ersparen sich die mühsame Konfiguration von Filterrichtlinien, bei denen die Gefahr besteht, dass sie zu viel blockieren (und die Produktivität der Nutzer einschränken) oder zu wenig blockieren (und Bedrohungen durchlassen).

Beispielhafter Anwendungsfall: Deferred Phishing stoppen

Problem: Deferred Phishing entzieht sich der Erkennung

Mit der richtigen Taktik und Motivation können Deferred Phishing-Kampagnen die herkömmlichen Schutzmaßnahmen umgehen.

Kampagnen-Setup: Angreifer können damit beginnen, eine authentisch aussehende E-Mail von einer neu erstellten Domain zu versenden, die eine ordnungsgemäße E-Mail-Authentifizierung (SPF, DKIM, DMAR) und eine harmlose Webseite verwendet.

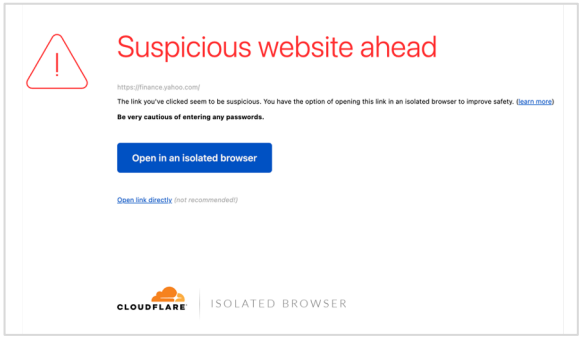
Erfolgreiche Zustellung im Posteingang: Diese E-Mails können sich der Erkennung durch sichere E-Mail-Gateways, authentifizierungsbasierte Filter oder andere Dienste entziehen, die sich auf reputationsbasierte Signale und andere deterministische Techniken verlassen.

Umleitung auf einen schädlichen Link: Wenn die E-Mail erfolgreich zugestellt wurde, kann der Angreifer den Link auf ein bösartiges Ziel umleiten, indem er die vom Angreifer kontrollierte Webseite ändert. Ein gängiges Beispiel ist eine gefälschte Anmeldeseite, die dazu dient, Anmeldedaten zu sammeln.

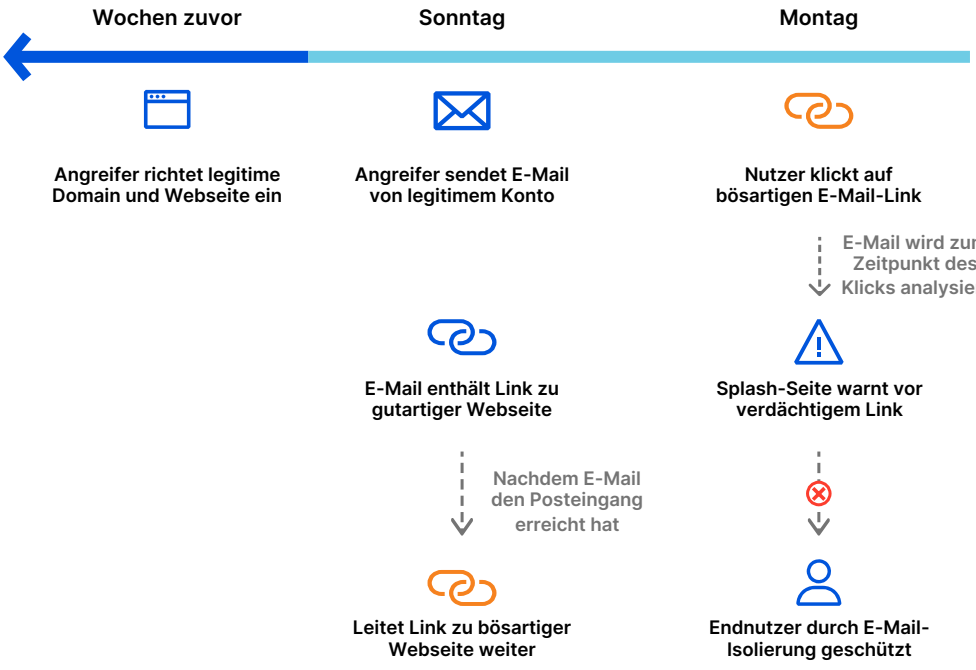
Lösung: Isolieren Sie verdächtige Links nach der Zustellung

Die Isolierung von E-Mail-Links bietet eine wichtige Schutzstufe nach der Zustellung. Cloudflare analysiert jeden Link in einer E-Mail, auf den ein Nutzer klickt. Wenn der Link als verdächtig oder riskant eingestuft wird, zeigt Cloudflare eine Warnseite an *(siehe unten)* und isoliert dann die Webseite, wenn der Nutzer sie anklickt.

Administratoren verhindern, dass bösartiger Code auf lokalen Geräten ausgeführt wird, und können Datenschutzkontrollen anwenden, z. B. das Hoch- und Herunterladen von Dateien einschränken, Tastatureingaben des Nutzers verhindern oder die Seite im schreibgeschützten Modus öffnen.



Zeitleiste einer Deferred Phishing-Kampagne



Cloudflare analysiert jeden Link zum Zeitpunkt des Klicks

Sicherer Link: Nutzer werden transparent auf diese Seite umgeleitet.

Schädlicher Link: Nutzer werden am Navigieren gehindert.

Verdächtiger Link: Nutzern wird stark davon abgeraten, zu navigieren, und sie werden mit einer Splash-Warnseite konfrontiert, die sie auffordert, den Link in einem isolierten Browser zu betrachten.

Integration von Cloud-E-Mail-Sicherheit mit Cloudflare Zero Trust

Moderne Sicherheit mit Zero Trust

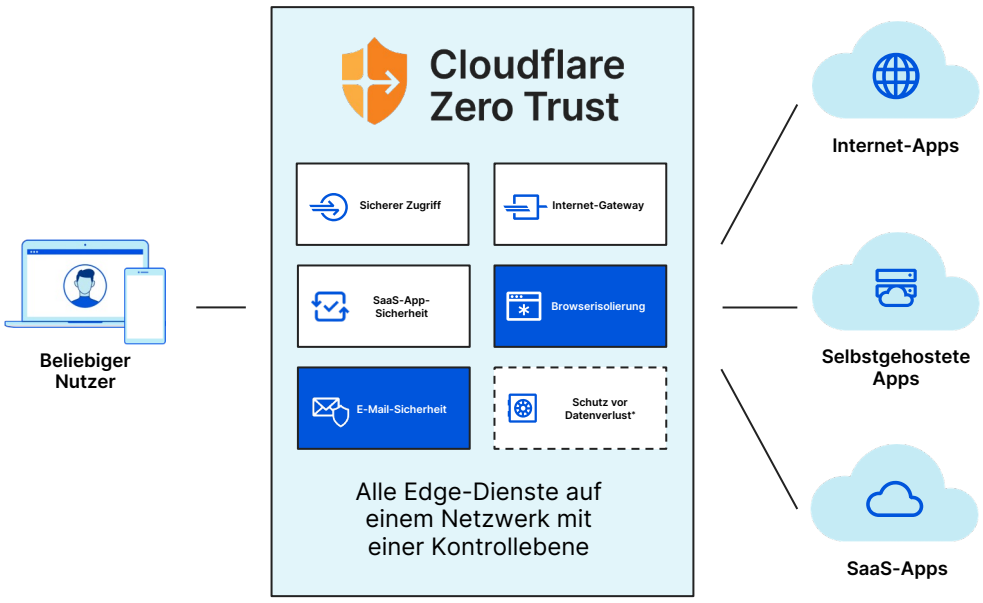
Cloudflare Zero Trust erhöht die Transparenz, verringert die Komplexität und senkt das Risiko beim Anwendungs- und Internetzugriff durch Beschäftigte, ob von zu Hause oder im Büro.

Am 1. April 2022 schloss Cloudflare die Übernahme von Area 1 Security ab. Unser Ziel ist es, den Schutz der Nutzer vor Phishing-Angriffen in E-Mail-, Web- und Netzwerkumgebungen durch unsere Zero Trust-Plattform zu verbessern. Lesen Sie hier mehr.

E-Mail-Sicherheit: Kernstück von Zero Trust

Cloudflare Area 1 E-Mail-Sicherheit verbessert Zero Trust, indem es implizites Vertrauen aus E-Mails entfernt, um Phishing- und BEC-Angriffe (Business Email Compromise) präventiv zu stoppen.

Vertrauen Sie niemals einem Absender, auch wenn er intern ist. Stellen Sie stattdessen sicher, dass der gesamte Datenverkehr der Nutzer, einschließlich E-Mails, überprüft, gefiltert, inspiziert und von Internet-Bedrohungen isoliert wird. Die E-Mail-Sicherheit wird in die Zero Trust-Services von Cloudflare integriert, gebündelt mit leistungsstarken Features wie RBI, CASB und mehr.



VPN-Ersatz
vereinfacht und sichert die Verbindung zwischen jedem Benutzer und jeder Ressource

Internetschutz
Schützen Sie Ihre Daten vor Bedrohungen über jeden Port und jedes Protokoll

Optimieren Sie die SaaS-Sicherheit
Sichtbarkeit und Kontrolle von Anwendungen einschließlich E-Mail

Modernisierung der Sicherheit
verbesserte Produktivität, einfachere Abläufe, geringere Angriffsfläche

* Tragen Sie sich in unsere DLP-Warteliste

Cloud-E-Mail-Sicherheit (CES)

- Reduzieren Sie die Reaktionszeiten auf Phishing-Vorfälle um 90%.
- Identifizieren Sie die Infrastruktur und die Übermittlungsmechanismen der Angreifer im Voraus, um Phishing in den frühesten Stadien des Angriffszyklus zu stoppen.
- Entfernen Sie implizites Vertrauen aus E-Mails, indem Sie den Inhalt, den Kontext und die sozialen Graphen der Kommunikation analysieren.
- Nutzen Sie Integrationen mit Microsoft, Google und anderen Umgebungen, um die integrierte Sicherheit zu verbessern.

Remote Browser Isolation (RBI)

- Stoppen Sie die Kompromittierung von Zugangsdaten, indem Sie riskante Websites im „Read-Only-Modus“ öffnen und die Interaktionen der Nutzer kontrollieren (z.B. Tastatureingabe, Kopieren & Einfügen, Up-/Download).
- Führen Sie den gesamten Browser-Code über das Netzwerk von Cloudflare aus und isolieren Sie so lokale Geräte von bösartigem Code.
- Sorgen Sie für ein reibungsloses, schnelles Erlebnis für den Nutzer. Anstelle des typischen Pixel-Streamings zeigen wir eine exakte Nachbildung der Seite von einem entfernten Browser, der nur <50 ms von 95 % der Nutzer weltweit entfernt ist.

Jetzt Analyse des Phishing-Risikos anfordern

Kontakt

+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

REV: PMM-2022JUN

[1] *Gartner Hype Cycle for Network Security, 2021* / GARTNER und HYPE CYCLE sind eingetragene Handels- und Dienstleistungsmarken von Gartner, Inc. und/oder den Tochtergesellschaften des Unternehmens in den USA und anderen Ländern, die im Folgenden mit Genehmigung verwendet werden. Alle Rechte vorbehalten.