AKAMAI-PRODUKTBESCHREIBUNG

Secure Internet Access ThreatAvert

Schutz wichtiger Netzwerkassets und Erkennung von Malware, die sich auf Ihre Kunden auswirken kann

Als Serviceanbieter wissen Sie, dass die Netzwerksicherheit den Markenwert beeinflusst, da sie sich direkt auf die Nutzerzufriedenheit auswirkt. Die meisten Bedrohungen verlassen sich auf das DNS – und es werden neue Bedrohungen entwickelt, die speziell auf die kritische DNS-Infrastruktur abzielen. Anbieter müssen ihre Maßnahmen zum Schutz von Netzwerkressourcen und Kunden überdenken, insbesondere da Bedrohungen immer dynamischer und vielfältiger werden – und das in einer rundum vernetzten Welt.

Akamai Secure Internet Access ThreatAvert untersucht DNS-Lookups in Echtzeit, um schädliche Aktivitäten zu erkennen und zu unterbinden. Secure Internet Access ThreatAvert wehrt Bedrohungen ab, die Netzwerkausfälle oder Verlangsamungen verursachen, sich negativ auf das Nutzererlebnis auswirken oder den Netzwerkschutz beeinträchtigen. Hierzu zählen beispielsweise folgende Bedrohungen:

- DNS-basierte DDoS-Angriffe, durch die Resolver mit riesigen Abfragemengen überlastet werden
- Bot-Malware, durch die wertvolle personenbezogene Daten gestohlen oder Verbrauchergeräte infiziert werden
- DNS-Tunnel, durch die Services durch Übertragung anderer Protokolle in das DNS gestohlen werden

Secure Internet Access ThreatAvert basiert auf dem führenden CacheServe-DNS-Resolver von Akamai und umfasst dynamische GIX-Bedrohungsfeeds. Dank jahrelanger Investitionen zur Optimierung der Performance und zahlreicher Softwareverbesserungen zur Gewährleistung von Widerstandsfähigkeit und Verfügbarkeit bietet CacheServe perfekte Zuverlässigkeit auch bei großem DNS-Trafficvolumen. Akamai Threat Intelligence wurde durch das Akamai Data Science-Team entwickelt, das mehr als 100 Milliarden DNS-Abfragen verarbeitet, die täglich in Echtzeit aus der ganzen Welt eingehen.

DNS-Schutz muss auf den DNS-Servern erfolgen

DNS-Abfragen sind ein beliebter Indikator schädlicher Aktivitäten, da die Auflösung der Adresse einer schädlichen Quelle, wie z. B. Command and Control-Server, Malwaredownloads, Extraktionssites usw., in den meisten Fällen den ersten Schritt zur Durchführung schädlicher Aktivitäten darstellt. DNS-Resolver sind der ideale Ort, um Bedrohungsinformationen zu implementieren, da sie alle Abfragen in einem Anbieternetzwerk einsehen. Schädliche Aktivitäten werden hierbei erkannt, indem eingehende Abfragen anhand von Einträgen in dynamischen Bedrohungslisten überprüft werden.

VORTEILE FÜR IHR UNTERNEHMEN

- Schlanke Lösung, Skalierung für Millionen Abonnenten, Abdeckung aller Geräte
- Führende Data Science für überragende Bedrohungsabdeckung
- Fortlaufend aktualisierte Bedrohungsfeeds, die Schutz vor neuen Exploits bieten
- Intuitive Echtzeitberichte mit einem schnellen Überblick über den Bedrohungsstatus und Links zu mehr Details
- Effiziente Erfassung und skalierbare Verwaltung von Bedrohungs- und Telemetriedaten

Die Skalierung von Secure Internet Access ThreatAvert betrifft die DNS-Steuerebene, sodass die Lösung deutlich weniger Kosten, Aufwand und Netzwerkbeeinträchtigung verursacht als dedizierte Lösungen zur Paketverarbeitung, die mit Traffic auf Datenebene skalieren.

Die Lösung ist schlank und effizient, und der Netzwerktraffic verursacht keine zusätzliche Latenz. Da sie netzwerkbasiert funktioniert, ist jedes Gerät abgedeckt. Clients und Hosts müssen Sicherheitssoftware weder installieren noch aktualisieren.

Überragende Präzision und optimaler Umfang der Bedrohungsabwehr

Cyberkriminelle entwickeln ihre Malware ständig weiter, um den ROI für ihre Exploits zu maximieren. Deshalb gestalten sie die Bedrohungen so, dass sie der Erkennung entgehen und sich ggf. schnell verändern können, um weiterhin zu funktionieren. Auch die Angriffsfläche wird durch die riesige Anzahl an IoT-Geräten (Internet of Things) stetig erweitert, sodass Angreifer auf verschiedenste Methoden zurückgreifen können, um ihre Ziele zu erreichen.

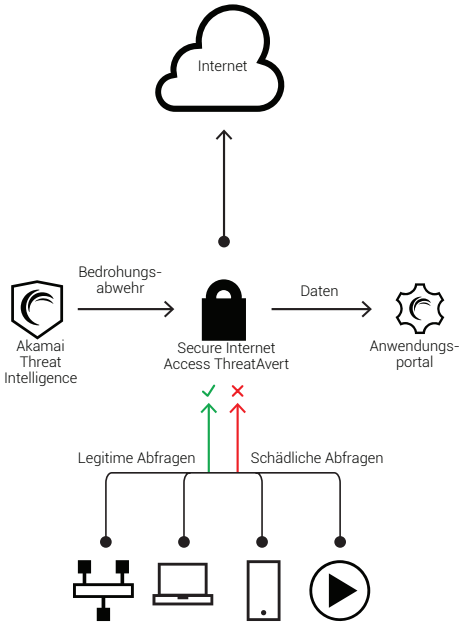
Angesichts der Raffinesse und Vielfalt der Bedrohungslandschaft hat das Data Science-Team von Akamai wichtige Systeme zur Analyse von in Echtzeit übertragenen DNS-Abfragen entwickelt und implementiert. Drittanbieterdaten aus Reputationslisten, Honeypots und andere Drittanbieterquellen sind in den Prozess integriert. Der überragende Umfang der Bedrohungsabwehr sowie die Präzision und die Agilität sind auf Investitionen in folgende Bereiche zurückzuführen:

- Zum Patent angemeldete Algorithmen zur sofortigen Erkennung von Verhaltensanomalien (wie z. B. bei DNS-DDoS-Angriffen), Korrelation verschiedener Bedrohungen und Erkennung neuer Bot-DGAs (Domain Generation Algorithms)
- Fortschrittliche Techniken für das automatische Erlauben von Namen, um zu gewährleisten, dass legitime DNS-Abfragen immer geschützt sind
- Forschungsmitarbeiter mit jahrelanger Erfahrung im Bereich Sicherheit und fundiertem Wissen zu Malware und DNS-Daten
- Weltweites Netzwerk und globale Rechenzentren für Echtzeitverarbeitung von Datenstreams

Präzise Richtlinien blockieren schädlichen Traffic und schützen legitimen Traffic

In Akamai Threat Intelligence-Feeds sind präzise Richtlinien integriert, mit denen unerwünschter DNS-Traffic verwaltet wird. Mithilfe vielfältiger Funktionen können Sie detaillierte Filter einstellen, um Malwareabfragen abzuwehren und gleichzeitig legitime Abfragen zu schützen bzw. zu beantworten:

- Präzise Richtlinien können auf eingehende Abfragen und ausgehende Antworten angewendet werden.
- Filter und Ratenbeschränkungen können basierend auf IP, QTYPE, FQDN und vielen anderen Abfrageparametern festgelegt werden.
- Filter und Ratenbeschränkungen können mehrere Abfrageparameter sowie logische Operatoren verwenden, wie z. B. „QTYPE AND FQDN“ oder „IP AND FQDN“.



Die zahlreichen von Akamai-Experten verarbeiteten Daten schaffen eine umfassende Übersicht zu schädlichen Aktivitäten im gesamten Internet und zu lokalen Angriffen.

- Filter und Ratenbeschränkungen können anhand dynamischer Listen mit Bedrohungsinformationen oder vom Betreiber bereitgestellter Listen überprüft werden.
- Richtlinien und Bedrohungslisten lassen sich kombinieren: MATCH: BLOCKLIST, NOT: ALLOWLIST
- Verschiedene Richtlinienaktionen bestimmen, wie Abfragen verarbeitet werden: ignorieren, Antwort synthetisieren, mit Abschneiden antworten, NXD, NOERROR und viele mehr.
- Richtlinien lassen sich kombinieren und verschachteln, sodass Sie sie optimal nutzen können.

Präzise Richtlinien können auch manuell konfiguriert werden, um lokale Probleme in einem Anbieternetzwerk zu beheben.

Skalierbares Datenmanagement, umfassende Telemetrie und umfangreiches Reporting

Secure Internet Access ThreatAvert beinhaltet eine Datenmanagement-Architektur, die auf offenen Lösungen basiert. Diese Lösungen haben sich bereits in den weltweit größten Netzwerken bewährt und ermöglichen einen optimalen Onlinebetrieb mit der nötigen Skalierung und Geschwindigkeit. Die in Echtzeit von den ThreatAvert-Systemen übertragenen Daten werden netzwerkweit zusammengefasst und dem Reporting (siehe unten) und anderen Systemen zur Verfügung gestellt. Die widerstandsfähige Architektur bietet unterbrechungsfreie Verfügbarkeit für ein optimales Kundenerlebnis. Und mit optionalen Connectors zu offenen Big-Data-Systemen (Splunk, Hadoop) oder speziellen Anwendungen können Sie zusätzliche Einblicke in Betrieb, Sicherheit und Geschäftsmetriken gewinnen.

Secure Internet Access ThreatAvert-Berichte bieten eine direkte Beurteilung der Sicherheitslage – mit einem zusammenfassenden Dashboard, das blockierte DNS-Abfragen, eingesparte Spitzenlasten bei der DNS-Bandbreite, am meisten verbreitete Malware im Netzwerk, Abonnenten mit infizierten Systemen und Threat-Intelligence-Updates anzeigt. Das zusätzliche Sicherheits-Dashboard enthält Diagramme mit DDoS- und Malwareinformationen. Und mit einem Klick lassen sich weitere Details zu Malware und infizierten Clients abrufen. Sie können in wenigen Minuten eigene Dashboards und Berichte erstellen, um Sicherheitsdaten in einem nutzerdefinierten Format zu erstellen – ganz nach Ihren betrieblichen Anforderungen. Über Tag-basierte Berichte können Bediener eigene Ansichten ihrer Secure Internet Access ThreatAvert-Topologie konfigurieren, die genau die gewünschten Elemente enthalten.