

DNS- SICHERHEITSSERVICE – DATENSCHUTZ

Produktzusammenfassung

Der DNS-Sicherheitservice von Palo Alto Networks identifiziert Bedrohungen, die im Domain Name System-(DNS-)Datenverkehr verborgen sind. Dabei werden die Bedrohungsdaten und das maschinelle Lernen von Palo Alto Networks genutzt. Der Service verwendet vorausschauende Analysen, um Angriffe zu unterbinden, die das DNS für Command-and-Control-(C2-)Vorgänge oder für Datendiebstahl verwenden. Die enge Verzahnung mit Palo Alto Networks-Firewalls der nächsten Generation bietet automatisierten Schutz. Separate Tools sind nicht erforderlich.

Verarbeitung der DNS-Daten

Die Palo Alto Networks-Firewalls der nächsten Generation ermitteln mithilfe einer lokalen Suche, ob eine angeforderte Domain bekannt ist oder nicht. Ist eine Domain unbekannt, wird sie in die DNS-Security-Cloud weitergeleitet, wo durch den DNS-Sicherheitservice geprüft wird, ob sie in einer Domain-Datenbank vorhanden ist. Mithilfe von maschinellem Lernen werden die angeforderte Domain und der Kontext der Anforderung untersucht, um Muster zu identifizieren. Diese Muster können auf die Verwendung von DNS-Tunneling zur Verhinderung einer C2-Blockierung oder auf die Verwendung eines Domain-Generation-Algorithmus (DGA) zur Erzeugung mehrerer Domains hinweisen, mit denen eine Signaturblockierung umgangen werden soll. Wenn der DNS-Sicherheitservice eine bekanntermaßen schädliche Domain erkennt oder eine Domain, die einen DGA oder DNS-Tunneling nutzt, blockiert der Dienst diese Domain und kann den Datenverkehr stattdessen zu einer DNS-Sinkhole-Adresse umleiten, die vom Kunden eingerichtet wurde. Wenn der Datenverkehr an die Sinkhole-Adresse weitergeleitet wird, kann die Firewall Endpunkte identifizieren, die versuchen, schädliche Domains zu erreichen. Der DNS-Sicherheitservice erfasst keine personenbezogenen Informationen oder Informationen in Bezug auf die Endpunkte, von denen DNS-Anforderungen abgesetzt werden.

Zweck der Informationsverarbeitung durch den DNS-Sicherheitservice

Der DNS-Sicherheitservice von Palo Alto Networks verarbeitet Informationen, um den Zugriff auf bekannte schädliche Domains zu blockieren, Aktivitäten mit Hinweisen auf schädliche Domains zu identifizieren, den Datenverkehr zu diesen Domains zu blockieren und die Identifizierung infizierter Endpunkte durch die Firewall zu ermöglichen.

Rechenzentren

Die vom DNS-Sicherheitservice verarbeiteten Daten werden in den Rechenzentren von Palo Alto Networks und der Google Cloud Platform (GCP™) verwaltet, die der Firewall des Kunden am nächsten liegen.

Aufbewahrung

Palo Alto Networks speichert Informationen über Domains, die vom DNS-Sicherheitservice analysiert wurden. Allerdings betrifft dies nur Daten von öffentlich verfügbaren Domains, nicht von Domains, die vom Kunden intern gehostet werden.

Zugriff und Offenlegung

Zugriff durch Kunden

Die Kunden können auf die Informationen über schädliche Domains, die durch den DNS-Sicherheitservice festgestellt wurden, über die Panorama™-Schnittstelle für Netzwerksicherheitsmanagement direkt von der Firewall aus zugreifen.

Zugriff durch Palo Alto Networks

Der Zugriff auf Informationen im DNS-Sicherheitsservice ist auf Palo Alto Networks Site Reliability Engineers (SREs), auf Bedrohungserforschungs- und Analytikteams sowie bei der Öffnung eines Supportfalls auch auf Kundensupportteams beschränkt. Der Zugriff ist für die Fehlersuche, die Problemlösung und die Verbesserung der Effektivität von Sicherheitsmaßnahmen erlaubt. Jeder Zugriff wird aufgezeichnet und geprüft. Die Zugriffsberechtigungen werden durch die Leitung der Engineering-Abteilung verwaltet.

Ressourcen

Die folgenden Ressourcen enthalten weitere Informationen über DNS und zugehörige Palo Alto Network-Dienste:

- [Security Operating Platform](#)
- [Threat Prevention](#)

Über dieses Datenblatt

Bitte beachten Sie, dass die in diesem Datenblatt zur Verfügung gestellten Informationen, die technische oder fachliche Themen betreffen, nur der allgemeinen Kenntnisnahme dienen, sich ändern können und keinen rechtlichen oder fachlichen Rat darstellen. Eine Garantie für die Anwendbarkeit auf einen bestimmten Fall oder Konformität mit geltendem Recht ist nicht gewährleistet.



3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 89 89 087

www.paloaltonetworks.com

© 2019 Palo Alto Networks, Inc. Palo Alto Networks ist eine eingetragene Marke von Palo Alto Networks. Eine Liste unserer Markenzeichen finden Sie unter <https://www.paloaltonetworks.com/company/trademarks.html>. Alle anderen in diesem Dokument erwähnten Marken sind Markenzeichen der jeweiligen Unternehmen. dns-security-service-privacy-ds-052019