URL-Filtering

Phishing, Missbrauch von Anmeldedaten und Command-and-Control-Aktivitäten unterbinden – mit maschinellem Lernen

Durch bösartige Websites sind Mitarbeiter Phishingversuchen, möglichem Diebstahl von Anmeldedaten, Malwareangriffen und Ransomware ausgesetzt. Angreifer nutzen Automatisierung, um täglich Tausende von bösartigen neuen URLs zu generieren. Ältere Schutzmechanismen, zum Beispiel Standalone-Proxys oder Webfiltertools können da nicht mithalten. Bis bösartige Websites identifiziert, klassifiziert und ein Schutzmechanismus eingesetzt wurde, kann sich ein Angriff so weit ausbreiten, dass das ganze Unternehmen gefährdet wird. Einzelprodukte, die sich nicht mit Ihrem Sicherheitsstack integrieren lassen, sorgen dafür, dass Sie mehr Richtliniensätze verwalten müssen. Dadurch wird die Einführung neuer Geschäftsanwendungen verzögert. Gleichzeitig werden neue Ressourcen für die Instandhaltung benötigt.

Unternehmensvorteile

- **Entfernen von Security-Silos und Schutz der Benutzer:** Als native Komponente der ML-basierten NGFW bietet URL-Filtering erstklassige Websicherheit für Standorte, Zweigstellen und mobile Benutzer, unabhängig davon, wo sie sich gerade befinden. Auf schwer zu verwaltende ältere Lösungen können Sie in Zukunft verzichten.
- **Minimale operationelle Ausgaben:** URL-Filtering wird direkt in die bestehende Richtlinie für den Netzwerkdatenverkehr integriert, vereinfacht so das Regelwerk und vereinheitlicht die Verwaltung für die Sicherheitsteams.
- **Sperren neuer schädlicher Websites:** URL-Filtering kategorisiert und sperrt bisher unentdeckte schädliche URLs innerhalb von Millisekunden, bevor sie Ihr Netzwerk und Ihre Endbenutzer schädigen können.
- **Abwehr bekannter schädlicher Websites:** Schützen Sie Ihr Unternehmen vor bekannten webbasierten Bedrohungen. Dazu gehören Phishing, Malware, Exploit-Kits und Command-and-Control-Aktivitäten (C2).
- **Schutz vor Phishing:** Das Anmeldedatenphishing wird in Echtzeit unterbunden. Mehrere Sicherheitsebenen schützen Ihr Unternehmen vor bekannten und neuen Phishingwebsites.
- **Unterstützung bei der Einhaltung von Vorschriften und der zulässigen Nutzung:** Sorgen Sie dafür, dass Ihr Unternehmen interne, branchenspezifische und behördliche Richtlinien einhält.

Sicherer Internetzugang durch integrierten Schutz

Für einen sicheren Internetzugang benötigen Sie einen nativ integrierten Ansatz, der die Richtlinie für Ihre ML-basierte Next-Generation Firewall (NGFW) um einfach einzurichtende Web-Controls erweitert. Diese erkennen, verhindern und kontrollieren Bedrohungen automatisch. Das URL-Filtering von Palo Alto Networks geht über Whitelists und Blacklists für Websites hinaus. Die Funktion nutzt maschinelles Lernen, um neue und unbekannte Angriffe inline zu erkennen und abzuwehren, und sperrt Bedrohungen, bevor ein Benutzer darauf zugreifen kann.

Der Dienst analysiert URLs und stuft sie dann als harmlos oder schädlich ein. Diese Klassifizierung können Sie in die Richtlinien Ihrer ML-basierten NGFW implementieren und so zur lückenlosen Kontrolle des Datenverkehrs nutzen. Diese Kategorien lösen über die gesamte Firewallplattform hinweg komplementäre Funktionen aus und aktivieren so zusätzliche Sicherheitsebenen, zum Beispiel gezielte SSL-Entschlüsselung und erweiterte Protokollierung. Zusätzlich zu der eigenen Analyse nutzt das URL-Filtering geteilte Bedrohungsdaten aus dem WildFire®-Malwareschutz und anderen Quellen. So werden die Schutzmechanismen gegen schädliche Websites automatisch aktualisiert.

Wichtige Funktionen

Erkennung durch maschinelles Lernen

Unser Abonnementservice für URL-Filtering stoppt neue Bedrohungen, bevor Benutzer darauf zugreifen können. Durch die Einbindung von maschinellem Lernen in Ihre ML-basierte NGFW werden ganz neue Phishing- und JavaScript-Angriffe inline unterbunden. Diese können sich dann nicht auf das ganze Unternehmen ausweiten. Bösartige URLs werden identifiziert und abgewehrt, bevor sie Ihr Unternehmen schädigen können.

Lückenlose Kontrolle von Webcontent

Die Internetrichtlinie ist eine Erweiterung Ihrer Firewall-richtlinie. Ihre ML-basierte NGFW verwendet URL-Filtering, um URL-Kategorien zu identifizieren, Risikowerte zu bestimmen und die Richtlinie einheitlich anzuwenden. Unterschiedliche URL-Kategorien und Risikowerte können mithilfe von differenzierten Richtlinien kombiniert werden. Dies ermöglicht eine ausnahmebasierte Anwendung, eine vereinfachte Verwaltung und eine präzise Kontrolle des Datenverkehrs über eine einzige Richtlinientabelle. Sie können gefährliche Websites sperren, die für Phishingangriffe, die Bereitstellung von Exploit-Kits oder C2 verwendet werden können. Gleichzeitig haben Ihre Mitarbeiter weiterhin die Möglichkeit, auf Webressourcen zuzugreifen, die sie für geschäftliche Zwecke benötigen.

Selektive Entschlüsselung von Datenverkehr

Durch eine gezielte Entschlüsselung können Sie das Risiko weiter verringern. Sie können Richtlinien festlegen, um TLS-/SSL-verschlüsselten Datenverkehr selektiv zu entschlüsseln. Damit können Sie potenzielle Bedrohungen schneller erkennen, ohne dabei gegen die Datenschutzvorschriften zu verstoßen. Sie können beispielsweise festlegen, dass bestimmte URL-Kategorien, zum Beispiel soziale Netzwerke, webbasierte E-Mails oder Content Delivery Networks, entschlüsselt werden sollen. Transaktionen von und zu anderen Websitearten, zum Beispiel von Behörden, Bankinstituten oder Gesundheitsdienstleistern, bleiben dann weiterhin verschlüsselt. Mit einfachen Richtlinien lässt sich festlegen, dass die Entschlüsselung nur bei Inhalten mit hohen oder mittleren Risikowerten vorgenommen wird. Selektive Entschlüsselung sorgt für optimale Sicherheit unter Einhaltung vertraulicher Parameter für den Datenverkehr, die durch die Unternehmensrichtlinien oder externe Vorschriften festgelegt sind.

Verhinderung von Anmeldedatenphishing

Schützen Sie Anmeldedaten und Passwörter in Echtzeit. URL-Filtering analysiert Websites auf Hinweise von Anmeldedatenphishing und ordnet sie in die URL-Kategorie „Phishing“ ein, sodass der Zugriff gesperrt wird. URL-Filtering ist eine echte Branchenneuheit. Die Funktion entdeckt und verhindert laufende Phishingangriffe und wehrt den Diebstahl von Anmeldedaten ab. Das geschieht durch die Kontrolle von Websites, bei denen Benutzer Anmeldedaten des Unternehmens auf Grundlage der URL-Kategorie der Website übermitteln können – ohne falsch-positive Ergebnisse. So können Sie verhindern, dass Benutzer ihre Anmeldedaten auf nicht vertrauenswürdigen Websites eingeben. Das Eingeben von Anmeldedaten auf Unternehmens- oder erlaubten Websites ist aber weiterhin möglich.

Anpassbare Kategorien

Passen Sie Kategorien und Richtlinien individuell für Ihr Unternehmen an. Beim URL-Filtering gibt es vorher festgelegte Kategorien. Manche Unternehmen haben aber unterschiedliche Ansprüche, wenn es um Risikotoleranz, Compliance, Richtlinien oder zulässige Nutzung geht. Damit die Sicherheitsrichtlinien genau zu Ihrem Unternehmen passen, können Ihre Administratoren benutzerdefinierte Kategorien erstellen, indem sie bereits vorhandene Kategorien kombinieren. Wenn Sie beispielsweise die Kategorien „high-risk“, „financial-services“ und „newly-registered-domain“ kombinieren, erhalten Sie eine wirksame neue Kategorie, bei der die Richtlinie auf jeder Website greift, bei der diese Kategorien vorhanden sind.

Analyse zwischengespeicherter Ergebnisse und Filtern von Übersetzungswebsites

Behalten Sie die Kontrolle über häufige Taktiken zur Richtlinienumgehung. URL-Filtering-Richtlinien können auch dann durchgesetzt werden, wenn bei Angriffen bekannte Umgehungstaktiken zum Einsatz kommen, zum Beispiel bei zwischengespeicherten Ergebnissen und Übersetzungswebsites. Dabei kommen folgende Elemente zum Einsatz:

- **Abwehr von in Suchmaschinen zwischengespeicherten Ergebnissen:** Die URL-Filtering-Richtlinien werden angewendet, wenn Endbenutzer versuchen, zwischengespeicherte Ergebnisse aus Internetsuchen oder -archiven anzusehen.
- **Filterung von Übersetzungswebsites:** Die URL-Filtering-Richtlinien werden angewendet, wenn URLs auf einer Übersetzungswebsite wie Google Translate eingegeben werden, um so die Richtlinien zu umgehen.

Safe Search Enforcement

Mit Safe Search Enforcement können Sie verhindern, dass unangemessene Inhalte in den Suchergebnissen der Benutzer angezeigt werden. Wenn diese Funktion aktiviert ist, werden nur Google-, Yandex- oder Bing-Suchen mit den strengsten Optionen für eine sichere Suche zugelassen. Alle andere Suchen können gesperrt werden.

Anpassbare Endbenutzerbenachrichtigungen

Jedes Unternehmen hat eigene Anforderungen für die Benachrichtigung von Benutzern, die versuchen, Webseiten aufzurufen, die gemäß den Richtlinien und dem zugehörigen URL-Filtering-Profil gesperrt sind. Administratoren können Benutzer mit einer individuellen Sperrseite über den versuchten Verstoß informieren. Diese enthält Angaben zum Benutzernamen

und zur IP-Adresse, die URL, auf die zugegriffen werden sollte, und die URL-Kategorie der Seite sowie eine selbst verfasste Nachricht des Administrators. Um die Verantwortung für die Aktivitäten im Internet zumindest teilweise wieder an die Benutzer zu übertragen, stehen Administratoren zwei Optionen zur Verfügung:

- **Fortfahren:** Es wird eine benutzerdefinierte Warnseite mit einem Button zum Fortfahren angezeigt. Die Benutzer können so auf Risiken hingewiesen werden, die die angeforderte Website birgt, und können dann selbst entscheiden, ob sie das Risiko als annehmbar einschätzen.
- **Außerkraftsetzung:** Bei dieser Option muss der Benutzer ein konfigurierbares Passwort eingeben, um eine Ausnahme der Richtlinie zu erstellen. Erst dann kann er fortfahren. Somit ist der Zugriff auf potenziell kritische Websites nur mit Zustimmung des Administrators möglich.

Die Effizienz der Palo Alto Networks-Sicherheitsabonnements

In letzter Zeit haben Cyberangriffe an Umfang und Komplexität zugenommen, wobei fortschrittliche Methoden zur Umgehung von Netzwerksicherheitsgeräten und -tools verwendet werden. Dies stellt Unternehmen vor die Herausforderung, ihre Netzwerke zu schützen, ohne die Arbeitslast der Sicherheitsteams zu erhöhen oder die Produktivität des Unternehmens zu mindern. Unsere cloudbasierten Sicherheitsabonnements, die nahtlos in die branchenweit erste ML-basierte NGFW-Plattform integriert sind, koordinieren die Informationen und bieten Schutz vor allen Angriffsvektoren, verfügen über erstklassige Funktionalität und eliminieren gleichzeitig die Lücken, die durch einzelne Netzwerksicherheitstools entstehen. Nutzen Sie die Vorteile marktführender Funktionen mit der konsistenten Erfahrung einer Plattform, und schützen Sie Ihr Unternehmen vor selbst den fortschrittlichsten und evasivsten Bedrohungen. Vorteile von URL-Filtering und anderen Sicherheitsabonnements:

- **Abwehr von Bedrohungen:** Gehen Sie über herkömmliche IPS-Lösungen (Intrusion Prevention System) hinaus und verhindern Sie automatisch alle bekannten Bedrohungen des gesamten Datenverkehrs in einem einzigen Verfahren.
- **WildFire:** Unbekannte Malware wird durch branchenführende, cloudbasierte Analysen automatisch erkannt und abgewehrt, um die Sicherheit von Dateien zu gewährleisten.
- **DNS-Sicherheit:** Unterbrechen Sie Angriffe, die DNS für C2-Aktivitäten und Datendiebstahl nutzen, ohne dass Änderungen an Ihrer Infrastruktur erforderlich sind.
- **IoT-Sicherheit:** Schützen Sie IoT- und OT-Devices in Ihren Unternehmen mit der ersten einsatzbereiten IoT-Sicherheitslösung der Branche.
- **GlobalProtect™**-Netzwerksicherheit für Endpunkte: Erweitern Sie die ML-basierten NGFW-Funktionen auf Ihre Remotebenutzer, um überall in Ihrer Umgebung konsistente Sicherheit zu gewährleisten.

Unternehmensvorteile

Ein URL-Filtering-Abonnement bringt folgende Vorteile mit sich:

- **Daten aus unterschiedlichen Quellen:** Nutzen Sie die branchenführende Websicherheitslösung mit einfachen anwendungs- und benutzerbasierten Richtlinien sowie einer lückenlosen Integration mit Threat Prevention und WildFire.
- **Lückenlose Kontrolle des Datenverkehrs:** Verwenden Sie URL-Kategorien, um automatisch fortschrittliche Sicherheitsmaßnahmen auszulösen, zum Beispiel selektive TLS-/SSL-Entschlüsselung verdächtiger Seiten.
- **Automatisierte Sicherheit:** Die Richtlinie wird automatisch auf die URL-Kategorien angewendet. Eingriffe von Analysten sind nicht erforderlich.
- **Insights über Benutzer- und URL-Aktivitäten:** Ihre IT-Abteilung behält mithilfe von vordefinierten oder selbst angepassten URL-Filtering-Berichten den Überblick über das URL-Filtering und die zugehörigen Webaktivitäten.

Tabelle 1: Erstellung von Richtlinien basierend auf URL-Kategorien*

Richtlinien	Beschreibung
Selektive SSL	Einleitung der SSL-Entschlüsselung basierend auf URL-Kategorien
Diebstahl von Anmeldedaten	Identifizierung von Websites, die Anmeldedaten des Unternehmens empfangen dürfen, und Sperrung, Zulassung oder Warnmeldung, wenn Benutzer versuchen, Anmeldedaten an nicht autorisierte Websites zu übermitteln
Sperren besonders riskanter Dateitypen	Unterbinden des Hoch- bzw. Herunterladens ausführbarer Dateien oder potenziell gefährlicher Dateitypen
Striktere IPS-Profile	Automatische Anwendung strikterer Profile gegen Sicherheitslücken und Spyware für bestimmte URL-Kategorien, um Phishing-Kits, Exploit-Kits und server- und clientseitige Sicherheitslücken zu blockieren
Benutzerbasierte Richtlinien	Identifizierung ausgewählter Gruppen in Unternehmen, die auf bestimmte, für alle anderen Mitarbeiter gesperrte URL-Kategorien zugreifen dürfen

*Neben dem generellen Sperren schädlicher Websites können URL-Kategorien auch zur Einrichtung nuancierter Sicherheitsrichtlinien genutzt werden, um Benutzer zu schützen, ohne dabei den Geschäftsbetrieb zu beeinträchtigen.

Tabelle 2: Zusammenfassung Datenschutz und Lizenzierung	
Datenschutz mit URL-Filtering-Abonnement	
Vertraulichkeit und Datenschutz	Palo Alto Networks verfügt über strenge Datenschutz- und Sicherheitskontrollen, um unbefugten Zugriff auf sensible oder persönlich identifizierbare Informationen zu verhindern. Wir wenden branchenübliche Best Practices für Sicherheit und Vertraulichkeit an. Zusätzliche Informationen finden Sie in unseren Datenblättern zum Datenschutz.
Lizenzierung und Anforderungen	
Anforderungen	Zur Nutzung des URL-Filtering-Abonnements von Palo Alto benötigen Sie Folgendes: • Palo Alto Networks Next-Generation Firewalls mit PAN-OS 8.1 oder später • Palo Alto Networks Threat Prevention-Lizenz
Empfohlene Umgebungen	Palo Alto Networks Next-Generation Firewalls, die an beliebigen Standorten eingesetzt werden, da Bedrohungen durch Phishing, Diebstahl von Anmeldedaten und C2 eine externe Verbindung benötigen.
URL-Filtering-Lizenz	URL-Filtering erfordert eine Standalonelizenz, die als integriertes, cloudbasiertes Abonnement für Palo Alto Networks Next-Generation Firewalls bereitgestellt wird. Es ist auch im Rahmen der Palo Alto Networks Subscription ELA, der VM-Series ELA oder Prisma Access erhältlich.

paloalto NETWORKS

3000 Tannery Way
Santa Clara, CA 95054

Zentrale: +1 408 75 34 000
Vertrieb: +1 866 32 04 788
Support: +1 866 898 9087

www.paloaltonetworks.com