Vorteile

Unsere auf maschinelles Lernen (ML) gestützte Inline-Abwehr nutzt Daten aus unseren WildFire- und URL-Filtering-Services und reduziert die Dauer von der Erkennung unbekannten Netzwerkverkehrs zur Abwehr auf praktisch null. So können Sie …

- neue Bedrohungen sofort stoppen, bevor sie Ihre Infrastruktur infizieren und sich möglicherweise ausbreiten.
- schädliche Dateien und Skripts sowie Phishing-angriffe ohne Beeinträchtigung der Benutzererfah-rung oder des Geschäftsbetriebs blockieren.
- vorhandene Investitionen in Palo Alto Networks NGFWs, WildFire und URL-Filtering weiter nutzen.
- von einer nahtlosen, nativen Integration zwischen unseren NGFW- und Sicherheitsabonnements, zuverlässigem Schutz und einheitlicher Verwaltung profitieren und auf Sicherheitstools anderer Anbieter verzichten.
- Ihre Abwehr zukunftssicher machen und selbst die neuesten Angriffe abwehren.

Warum jede Sekunde zählt

Inline-Abwehr unbekannter Bedro-hungen mit maschinellem Lernen

Jedes Jahr kommen Millionen neuer Cyberbedrohungen auf, vor denen Unternehmen sich schützen müssen. Durch die Nutzung von Cloud-Ressourcen, Automatisierung und anderen Technologien sind Angreifer heute zunächst im Vorteil: Sie können ihre Exploits schneller denn je verbreiten und zudem polymorphe Malware und bösartige Inhalte einsetzen, die sich der Erkennung entziehen, indem sie ihre identifizierbaren Merkmale ständig verändern.

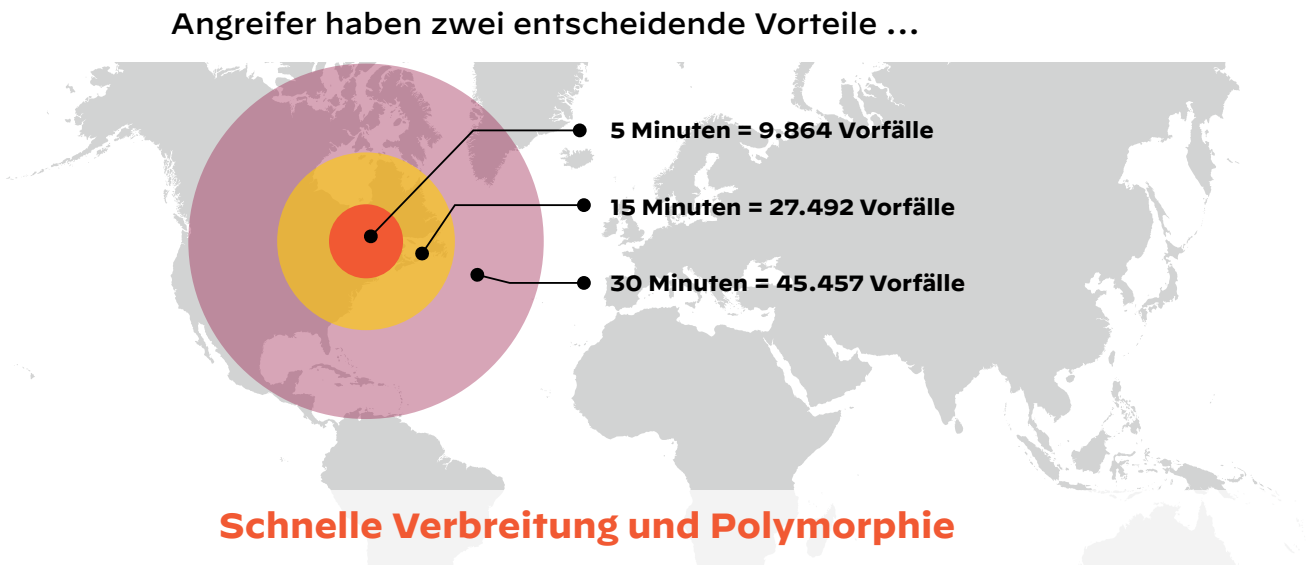

Abb. 1: Daten der Unit 42 von Palo Alto Networks zur Verbreitung von Malware

Angreifer sind auf dem Erfolgsweg. Allein im Jahr 2019 wurden mehr als 140 Millionen neue Malwareinstanzen identifiziert und täglich werden Tausende neuer schädlicher Websites und Domains erstellt. Neue Angriffe werden sehr viel schneller gestartet als herkömmliches Sandboxing, Proxys und unabhängige Signaturtechnologien Abwehrmaßnahmen ergreifen können. Nach einer erfolgreichen Erstinfektion kann moderne Malware in Sekundenschnelle Tausende weiterer Systeme infizieren – lange bevor Schutzmaßnahmen entwickelt und auf das Unternehmen ausgeweitet werden können.

Branchenkonzepte gegen neue Bedrohungen

Im Allgemeinen haben Unternehmen bislang auf vier Methoden zur Abwehr dieser neuen Angriffe zurückgegriffen.

Thors Hammer

Bei dieser Strategie gestatten die Unternehmensrichtlinien den Webzugriff auf Unternehmensressourcen und das Herunterladen von Dateien nur unter starken Einschränkungen oder gar nicht. In den meisten Fällen ist das natürlich nicht praktikabel und stört den Geschäftsbetrieb.

Überprüfen und freigeben

Bei diesem Ansatz werden jede einzelne Datei und jede Websiteanfrage zunächst angehalten und genau überprüft, bis die Risikofreiheit bestätigt werden kann. Auch diese Methode hat sich als wenig erfolgreich erwiesen. Das Aufhalten von Dateien beeinträchtigt die Produktivität und sorgt für eine negative Benutzererfahrung. Vor allem aber lässt sich dieses Vorgehen einfach nicht skalieren. Je mehr Dateien analysiert werden müssen, desto länger werden die Verzögerungen und desto schwerwiegender werden die Störungen für den Geschäftsbetrieb.

Unschädlich machen und rekonstruieren

Bei dieser Methode werden ausgewählte dokumentbasierte Dateiformate entweder in ein anderes Dateiformat konvertiert (um potenziell schädliche Inhalte unschädlich zu machen) oder in ihnen enthaltener Code ganz entfernt. Dabei geht oft die Formatierung verloren oder die Datei wird so beschädigt, dass sie sich nicht mehr öffnen lässt – ähnlich wie beim Öffnen von Office-Dokumenten im abgesicherten Modus oder beim Konvertieren ins PDF-Format. Aufgrund der aufwendigen Bearbeitung lässt sich auch dieser Ansatz nicht skalieren und wirkt sich negativ auf die Produktivität im Unternehmen und den Support aus. Außerdem werden so zwar dateibasierte Bedrohungen abgewehrt, aber keine webbasierten Bedrohungen.

Bekannte Bedrohungen inline abwehren und alles andere in der Cloud überprüfen

Diese Strategie verfolgen wir bei Palo Alto Networks. Damit geht der Betrieb ungestört weiter, aber wir haben Transparenz über den gesamten Netzwerkverkehr und können Abwehrsysteme automatisch aktualisieren, wenn ein Problem gefunden wird. So werden die Infektionsgefahr und die Beeinträchtigung der Benutzererfahrung minimiert. Da die Analyse des unbekannten Verkehrs offline erfolgt, ist der Ansatz auch skalierbar. Und weil die Analysekapazitäten sich in der Cloud befinden, können wir sie skalieren, kontinuierlich weiterentwickeln und neue Erkennungsfunktionen hinzufügen, ohne den Geschäftsbetrieb unserer Kunden zu stören.

Doch obwohl sich dieser Ansatz für unsere Kunden bewährt hat, war er uns noch nicht gut genug. Wir wollten einen Weg finden, Erstinfektionen durch völlig neue und unbekannte Bedrohungen möglichst schnell abzuwenden – idealerweise ganz ohne Verzögerung. Mit den neuen Funktionen in unserem Malwareschutzdienst WildFire® und dem URL-Filtering-Service ist uns das nun gelungen.

Abwehr unbekannter Bedrohungen mit Inline-ML

Palo Alto Networks hat die weltweit erste Next-Generation Firewall (NGFW) entwickelt, die mit Inline-ML unbekannte datei- und webbasierte Bedrohungen abwehrt. Mit unserem patentierten signaturunabhängigen Ansatz blockieren WildFire und URL-Filtering proaktiv schädliche Dateien und Skripts sowie

Phishingangriffe, ohne die Produktivität zu beeinträchtigen. Die Hardware und virtuellen NGFWs von Palo Alto Networks wenden neue ML-basierte Abwehrverfahren an:

- **WildFire (mit Inline-ML)** untersucht Dateien in Echtzeit und blockiert schädliche ausführbare Dateien sowie PowerShell®-Dateien, die den Großteil schädlicher Inhalte ausmachen.
- **URL-Filtering (mit Inline-ML)** untersucht unbekannte URLs in Echtzeit. Dabei lassen sich Phishingseiten und schädliche JavaScripts in Millisekunden erkennen und sofort stoppen, noch bevor sie ihr Ziel erreichen.

Bis zu 95 % aller datei- und webbasierten Bedrohungen können inline abgewehrt werden, ohne in den WildFire- oder URL-Filtering-Clouds analysiert werden zu müssen. Um den Rest kümmern sich Schutzmechanismen, die in Sekundenschnelle von den weltweit größten nativen Erkennungs- und Abwehr-Engines angewendet werden.

ML ist ein besonders wirkungsvolles Mittel zur Erkennung und Abwehr polymorpher Malwarevarianten und schnell mutierender webbasierter Bedrohungen und sollte daher unbedingt genutzt werden. Eine ML-basierte Engine, die in der Lage ist, große Datenmengen schnell zu verarbeiten, kann sofort Entscheidungen treffen und ermöglicht so eine schnelle Reaktion auf Bedrohungen, ohne erst auf die Ergebnisse gründlicher statischer, dynamischer oder anderer Analyseprozesse zu warten. Ein weiterer wichtiger Vorteil besteht darin, dass angewandte ML-Modelle Änderungen in ausführbaren Dateien besser erkennen können als signaturbasierte Methoden. Damit sind sie besser zur Erkennung von Malware geeignet, deren Autoren Methoden zur Erkennungsverhinderung eingesetzt haben.

Um ML wirksam einzusetzen, nutzen wir die riesigen Mengen an schädlichen Instanzen, globaler Telemetrie und Analysen aus unseren über die Cloud bereitgestellten WildFire- und URL-Filtering-Sicherheitsabonnements. Nach fast zehnjähriger Analyse und Bedrohungsdaten von Zehntausenden von Kunden und Partnern unterstützen diese einzigartigen Datenbanken die Modelle für maschinelles Lernen direkt und treiben die Entwicklung von Modellen voran, die klein und effizient genug sind, um inline eingesetzt zu werden und auf unseren ML-gestützten NGFWs in Echtzeit zu arbeiten.

Während Deep Intelligence und die zentrale zuverlässige Informationsquelle („Single Source of Truth“) in der Cloud bleiben, lassen sich Echtzeitentscheidungen und die Durchsetzung von Abwehrmaßnahmen an die NGFW verlegen, wo es am meisten auf Geschwindigkeit ankommt. Das kontinuierlich aktualisierte Cloud-Repository und die skalierte Verarbeitung ermöglichen es, bei Bedarf neue ML-Modelle zu erstellen. Dadurch wird sichergestellt, dass ML die neuen unbekannten Bedrohungen abwehrt, während neue Branchentrends und neue Arten von Bedrohungen entstehen. Die ML-basierten Inline-Maßnahmen blockieren die überwiegende Mehrheit neuer datei- und webbasierter Bedrohungen. Laufende und bewährte cloudbasierte Analysen mit schnellen Präventionsmöglichkeiten reduzieren das Zeitfenster für Angriffe auch für alle anderen Bedrohungen.

Funktionsweise: dateibasierte Angriffe

Das WildFire-Abonnement basiert auf Bedrohungsmodellen, die kontinuierlich in der Cloud verbessert werden, und ermöglicht eine ML-basierte Inline-Engine, die in unserer Hardware und innerhalb unserer virtuellen NGFWs bereitgestellt wird. Damit stoppen wir schädliche dateibasierte Inhalte wie z. B. ausführbare Dateien und gefährliche PowerShell-Angriffe ohne Dateien. Das geschieht vollständig inline und ohne Analyse in der Cloud. Die ML-Modelle werden täglich aktualisiert, sodass die Erkennungsfunktionen immer auf dem neuesten Stand sind.

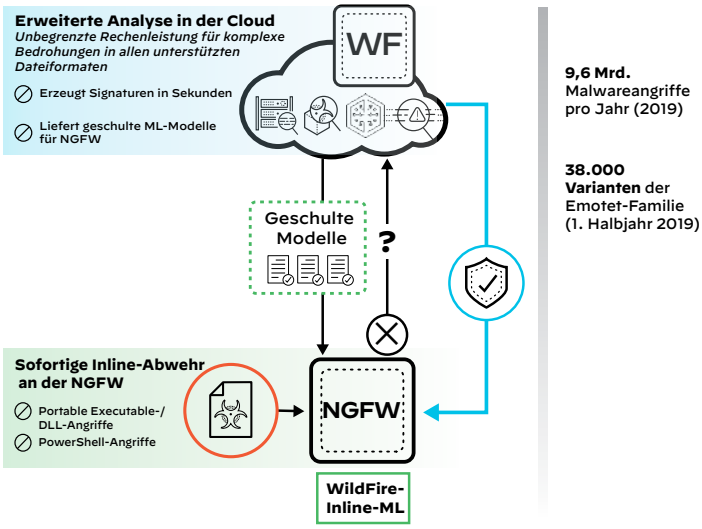

Abb. 2: ML-basierte Abwehr dateibasierter Angriffe

ML-basierte Abwehr wirkt sofort und leitet gescannte Dateien gleichzeitig zur Analyse an WildFire weiter. Dies schafft nicht nur eine Feedbackschleife für Fehlalarme, sondern beschleunigt auch die Prävention. Bedrohungen, die von der Inline-Prävention nicht erkannt werden würden (z. B. neue Bedrohungen in verschiedenen Formaten wie PDF- oder Office-/Microsoft 365™-Dateien, oder gut getarnte Bedrohungen, die für einen gezielten Angriff auf ein bestimmtes Unternehmen erstellt wurden), werden mit verzögerungsfreien Signaturaktualisierungen in Angriff genommen. Diese innovativen Signaturen werden kontinuierlich und in Echtzeit aus der Cloud geliefert, um schnelle Präventionsmaßnahmen durch cloudbasierte Prozesse nahezu in Echtzeit zu ermöglichen. Unabhängig davon, ob eine unbekannte Datei mit einer vorhandenen Signatur übereinstimmt oder von ML-Modellen an der NGFW klassifiziert wird, führt WildFire immer eine vollständige Analyse durch und extrahiert wertvolle Informationen und Daten, um Sicherheitsanalysten Kontext zu liefern, die ML-Modelle weiter zu schulen und den Austausch von Informationen mit anderen Abonnenten zu ermöglichen, um ähnliche Angriffe über andere Angriffsvektoren zu verhindern.

Funktionsweise: webbasierte Angriffe

Das URL-Filtering-Abonnement bringt ML direkt an die NGFW, damit neue, unbekannte Phishing- und JavaScript-Angriffe inline gestoppt werden, bevor sie ihr Ziel erreichen. Schädliche URLs werden in wenigen Millisekunden erkannt und sofort blockiert. URLs, die nicht als schädlich eingestuft werden, werden an die URL-Filtering-Cloud weitergeleitet und dort gründlich analysiert und kategorisiert. Dieser Vorgang dauert nur wenige Minuten.

Die Daten aus dem URL-Filtering-Service werden dazu genutzt, unsere ML-Modelle zu schulen und täglich zu aktualisieren. Die ML-basierte Abwehr webbasierter Angriffe stoppt neue schädliche URLs, bevor sie die Systeme von Benutzern infizieren können. Eine ausführliche Cloud-Analyse ermöglicht die umfassende

Kategorisierung, die sich dann in Ihr Onlinesicherheitssystem integrieren lässt.

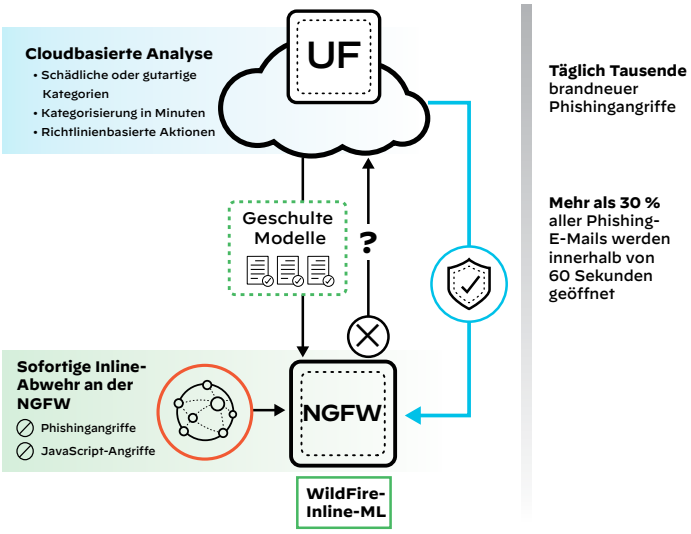

Abb. 3: ML-basierte Abwehr webbasierter Angriffe

Was spricht für Palo Alto Networks?

Prädiktive Modelle auf Basis unserer Cloud-Analyse

Wir sind wie kein anderer Anbieter in der Lage, unsere prädikativen ML-Klassifikatoren mit umfassenden Daten aufzubauen und weiterzuentwickeln. Einige der Datenquellen:

- **WildFire**, eine der größten weltweit verfügbaren, massiv skalierbaren und flexibel einsetzbaren Clouds zur Analyse von Malware.
- **URL Filtering**, ein cloudbasierter Dienst, der Bedrohungsdaten aus aller Welt in maschinelle Lernverfahren einspeist, um URLs zuverlässig zu kategorisieren und den Zugang zu Websites zu blockieren, die zur Verbreitung von Malware, für Command-and-Control-Kommunikation oder für schwer erkennbare Phishingmethoden genutzt werden.

Billionen von Dateien und URLs – sowohl harmlose als auch schädliche – wurden bereits von unserem verteilten Sensorsystem analysiert, das Daten von 52.000 Unternehmen, Behörden und Serviceprovidern sowie über 40 Partnern untersucht. Dieser einzigartige Bedrohungsdatensatz ermöglicht es Forschern und Datenwissenschaftlern von Palo Alto Networks, genaue und effiziente ML-Modelle zu erstellen, die ständig aktualisiert und automatisch an die NGFW geliefert werden, damit der Schutz immer auf dem neuesten Stand ist.

Weitere Ressourcen

- Datenblatt URL-Filtering
- Datenblatt WildFire
- Überblick: Künstliche Intelligenz und maschinelles Lernen in Sicherheitssystemen

Tabelle 1: Sicherheitsabonnements
Anforderungen
Für die Inline-ML-basierten Schutzmechanismen benötigen Sie:
• ML-gestützte Next-Generation Firewalls der VM-Series oder PA-Series mit PAN-OS® 10.0
• Aktive Abonnements für WildFire und URL-Filtering
• Firewalls mit konfigurierter Internetverbindung
Empfehlung
• Konfigurieren Sie die Firewalls so, dass sie Dateien an die WildFire-Cloud oder den URL-Filtering-Service übermitteln, damit die ML-Modelle optimiert und Fehlalarme gemanagt werden können.

Sicherheitsabonnements von Palo Alto Networks

Cyberangriffe haben an Umfang und Komplexität zugenommen und nutzen heute modernste Methoden zur Umgehung von Netzwerksicherheitsmechanismen. Das stellt Unternehmen vor die Herausforderung, ihre Netzwerke zu schützen, ohne die Arbeitsbelastung der Sicherheitsteams zu erhöhen oder die Produktivität im Unternehmen zu behindern. Unsere cloudbasierten Sicherheitsabonnements fügen sich nahtlos in unsere branchenführenden, ML-gestützten NGFWs ein, koordinieren die Daten und bieten Schutz für alle Angriffsvektoren. Sie bieten erstklassige Funktionen und vermeiden die Lücken, die beim Einsatz unterschiedlicher Netzwerksicherheitstools entstehen. Gleichzeitig profitieren Sie von marktführenden Funktionen und einer einheitlichen Plattform und schützen Ihr Unternehmen zuverlässig, sogar vor den komplexesten Bedrohungen. Es stehen verschiedene Sicherheitsabonnements zur Auswahl:

- **Threat Prevention:** Diese Lösung bietet mehr Sicherheit als ein herkömmliches IPS (Intrusion Prevention System), da automatisch alle bekannten Bedrohungen für den gesamten Datenverkehr in einem Durchlauf (Single Pass) abgewehrt werden.
- **WildFire:** Durch die automatische Erkennung und Abwehr unbekannter Malware mit branchenführenden cloudbasierten Analysen sind alle Dateien geschützt.
- **URL-Filtering:** Damit wird eine sichere Internetnutzung ermöglicht, da der Zugriff auf bekannte und neue schädliche Websites verhindert wird.
- **DNS Security:** Mit dieser Lösung werden Angriffe verhindert, die DNS als Command-and-Control-Kanal und für den Datendiebstahl nutzen. Dazu sind keine Infrastrukturänderungen erforderlich.
- **IoT Security:** Schützen Sie IoT- und OT-Geräte in Ihrem gesamten Unternehmen mit der ersten sofort einsatzbereiten IoT-Sicherheitslösung der Branche.
- Netzwerksicherheit für Endpunkte durch **GlobalProtect™**: Schützen Sie auch Telearbeiter mit den ML-gestützten NGFW-Funktionen und sorgen Sie so für konsistente Sicherheit in der gesamten Umgebung.

paloalto NETWORKS

Oval Tower, De Entrée 99-197
1101 HE Amsterdam, Niederlande

Telefon: +31 20 888 1883
Vertrieb: +800 723 9771
EMEA Support: +31 20 808 4600

www.paloaltonetworks.de