THREAT PREVENTION

Umfassender Schutz für Ihr Netzwerk vor Angriffen, Malware sowie Befehlstaktiken

Unternehmen sind ständigen Cyberattacken durch Angreifer auf der ganzen Welt ausgesetzt, die versuchen, auf diese Weise Profit zu erzielen. Angreifer sind heutzutage mit umfassenden finanziellen Mitteln und gutem technischen Equipment ausgestattet. Sie setzen auf Ausweichmanöver wie die Paketverschleierung, polymorphe Malware, Verschlüsselungstechnologien, mehrstufige Payload-Angriffe und Fast-Flux-DNS, um sich in einem Netzwerk einzunisten und dabei von traditionellen Netzwerk-Abwehrmaßnahmen unentdeckt zu bleiben.

Der von Palo Alto Networks® speziell in der Next-Generation-Sicherheitsplattform entwickelte Service zur Abwehr von Bedrohungen schützt Netzwerke während unterschiedlicher Angriffsphasen:

- Der gesamte Datenverkehr wird innerhalb des Kontextes von Anwendungen und Benutzern gescannt.
- Es werden Bedrohungen während jeder Phase des Lebenszyklus der Cyberattacke verhindert.
- Die Single-Pass-Scanning-Architektur ermöglicht einen hohen Durchsatz, ohne dabei die Sicherheit preiszugeben.
- Es werden täglich automatische Updates für neu entdeckte Bedrohungen bereitgestellt, die über den cloudbasierten Bedrohungsanalyse-Service von WildFire™ innerhalb von 300 Sekunden Schutzmechanismen für Zero-Day-Malware und Exploits bereitstellen.
- In technikgestützter Geschwindigkeit und Größenordnung werden revolutionäre automatisierte CnC-Signaturen erstellt.

Nach wie vor werden jedoch trotz der veränderten Bedrohungslandschaft bei den meisten Netzwerksicherheitsprodukten die bisher gängigen, aber mittlerweile unzureichenden Abwehrmechanismen eingesetzt. Der Datenverkehr wird nur auf bestimmten Ports kontrolliert. Während Abwehrmechanismen durch das Hinzufügen von Einzelfunktionsgeräten erweitert werden und so ein bestimmtes Problem gelöst werden kann, führt dies allgemein häufig zu einer schlechteren Erkennungsrate und Leistung. So entsteht durch Lücken in der Netzwerksicherheit und durch fragmentierte und schwer zu verwaltende Sicherheitslösungen ein Sicherheitsrisiko, das sich Angreifer vermehrt zunutze machen.

Anwendung aktivieren, Gefahren bannen

Anwendungen sind heutzutage aus dem Unternehmensumfeld nicht mehr wegzudenken. Immer häufiger erhalten Nutzer Zugriff auf diese Anwendungen, die über verschlüsselte Kanäle und nicht-standardisierte Ports den Weg in das Netzwerk nehmen. Um einen dauerhaften Zugriff zu gewährleisten wechseln Anwendungen durch Port-Hopping offene Ports nach dem Zufallsprinzip.

Diese Art und Weise, in der Anwendungen für Benutzer verfügbar gemacht werden, wird jedoch auch immer häufiger von Angreifern genutzt, um unentdeckt in ein Netzwerk einzudringen. Sie schleusen sich über Anwendungen ein, verwenden SSL-Tunnel und nutzen ahnungslose Ziele aus, um sich in einem Netzwerk einzunisten und schädliche Aktivitäten auszuführen.

Wir schützen Ihr Netzwerk durch mehrere Sicherheitsebenen vor diesen Bedrohungen, damit werden Bedrohungen in jeder Phase des Angriffs bekämpft. Neben konventionellen Funktionen des Eindringschutzes bieten wir die einzigartige Fähigkeit zur Erkennung und Blockierung von Bedrohungen auf allen Ports, anstatt Signaturen nur basierend auf einer begrenzten Anzahl von vordefinierten Ports aufzurufen. Durch den Einsatz von User-ID™ und App-ID™, den Technologien zur Benutzer- und Anwendungsidentifikation in unserer modernen Firewall, werden der Datenverkehr sowie der zugehörige Kontext auf allen Ports überwacht. Unsere Threat Prevention Engine behält mögliche Bedrohungen immer im Blick – unabhängig vom Ausweichmanöver, das sie nutzen.

Unser Threat Prevention-Abonnement umfasst Intrusion Prevention, Malwareschutz für Netzwerke sowie CnC-Schutzmechanismen (Command and Control).

Bedrohungen in jeder Phase ausschließen

Bei nahezu jeder Sicherheitsverletzung in der letzten Zeit setzte das betroffene Unternehmen nur eine Sicherheitslösung mit nur einem Schutzmechanismus ein, der vom Angreifer umgangen wurde.

- Bei der heuristischen Analyse werden ungewöhnliche Paket- und Datenverkehrsmuster wie Port-Scans, Host Sweeps und DDoS-Angriffe untersucht.
- Andere Schutzfunktionen, wie die Blockierung ungültiger oder fehlerhafter Pakete, IP-Defragmentierung und TCP-Zusammensetzung, werden zum Schutz vor gängigen Bedrohungen und Verschleierungsversuchen eingesetzt.
- Eine einfache Konfiguration und benutzerdefinierte Signaturen für Sicherheitslücken ermöglichen Ihnen eine gezielte Anpassung an die spezifischen Sicherheitsanforderungen in Ihrem Netzwerk.

Palo Alto Networks setzt nativ integrierte Schutzmechanismen ein um sicherzustellen, dass, falls bei einem Angriff ein Mechanismus versagen sollte, ein anderer Mechanismus greift. Der Schlüssel für einen effektiven Schutz ist die Verwendung von gezielt entwickelten Sicherheitsfunktionen, die nicht einfach nur den Datenverkehr untersuchen und Bedrohungen identifizieren und blockieren, sondern auch detaillierte Informationen liefern und teilen.

Intrusion Prevention (IPS):

Bedrohungsbasierte Sicherheitslösungen erkennen und blockieren Angriffsversuche sowie Umgehungsversuche wie Port-Scans, Pufferüberläufe, Ausführung von Remotecodes und Protokoll-Fragmentierung und Verschleierung auf Netzwerk- und Anwendungsebene. Die Schutzmechanismen basieren auf dem Abgleich von Signaturen und der Erkennung von Auffälligkeiten zur Dekodierung und Analyse von Protokollen. Gesammelte Informationen werden dann genutzt, um vor Gefahren und Angriffen zu warnen und diese zu blockieren. Über den Abgleich von Zustandsmustern können Angriffe unter Berücksichtigung der Reihenfolge und des Ablaufs erkannt werden. So wird sichergestellt, dass zugelassener Datenverkehr sicher ist und nicht zur Umgehung von Schutzmechanismen genutzt wird.

- Bei der Protokolldekoder-basierten Analyse wird das Protokoll zustandsabhängig analysiert und anschließend werden verschiedene Signaturen angewendet, um Netzwerk- und Anwendungs-Exploits zu erkennen.
- Da es verschiedene Möglichkeiten gibt, eine einzige Sicherheitslücke auszunutzen, basieren unsere Schutzsignaturen auf der Sicherheitslücke selbst. Dies ermöglicht einen besseren Schutz gegen eine Vielzahl von Exploits. Mit einer einzigen Signatur können so mehrere Angriffsversuche auf eine bekannte Schwachstelle im System oder in einer Anwendung verhindert werden.
- Beim Protokoll-Anomalien-basierten Schutz werden nicht mit RFC-konforme Protokollnutzungen wie überlange URI oder FTP-Logins untersucht.
- Eine einfache Konfiguration und benutzerdefinierte Signaturen für Sicherheitslücken ermöglichen uns eine gezielte Anpassung an die spezifischen Sicherheitsanforderungen in Ihrem Netzwerk.

Malware-Schutz

Der integrierte Malware-Schutz blockiert Malware, bevor sie überhaupt beim Ziel-Host eingeschleust werden kann, anhand von Signaturen, die auf einem Schadcode basieren, nicht auf einem Hash. Der Malwareschutz von Palo Alto Networks blockiert nicht nur bereits bekannte Malware, sondern auch neue und bisher unbekannte Varianten davon. Unsere Stream-basierte Suchengine schützt das Netzwerk, ohne spürbare Latenz für den Endbenutzer. Das ist ein entscheidender Vorteil gegenüber Netzwerk-Antiviruslösungen mit Proxy-basierten Suchengines. Der Stream-basierte Malwarescanner prüft den Datenverkehr, sobald die ersten Pakete einer Datei eingehen, und beseitigt Bedrohungen, ohne die bei herkömmlichen eigenständigen Lösungen üblichen Performanceeinbußen. Zu den wesentlichen Anti-Malware-Funktionen gehören:

- Integrierte und Stream-basierte Erkennung und Abwehr von in komprimierten Dateien und Webinhalten versteckter Malware.
- Schutz vor in gängigen Dateitypen wie Microsoft® Office®-Dokumenten und PDF-Dateien verstecktem Schadcode.
- WildFire-Updates stellen den Schutz vor Zero-Day-Malware sicher.

Palo Alto Networks sammelt Signaturen der unterschiedlichsten Malwaretypen von aktueller Schadsoftware, die sich im Umlauf befindet. Diese Sammlung wird ergänzt durch die Signaturen der bisher unbekannten und an WildFire, unser Unit42-Forschungsteam für Bedrohungen, und an andere führenden Forschungsorganisationen von Drittanbietern weltweit übermittelten Malware.

Command-and-Control (Spyware)-Schutz

Natürlich gibt es keinen Königsweg bei der Abwehr von Bedrohungen für ein Netzwerk. Wenn erst einmal Schadcode eingeschleust werden konnte, kommunizieren Angreifer mit dem Host-Rechner über einen Command-and-Control (CnC)-Kanal, um zusätzliche Malware

Nutzlast-basierte vs. Hash-basierte Signaturen

Signaturen, die auf Mustern zur Nutzlasterkennung im Dateiinhalt basieren, können zur Ermittlung von zukünftigen Variationen der Dateien genutzt werden, selbst wenn der Inhalt in geringem Umfang angepasst wurde. Auf diese Weise sind wir in der Lage, polymorphe Malware sofort zu erkennen und zu blockieren, die ansonsten wie eine neue unbekannte Datei behandelt worden wäre.

Hash-basierte Signaturen führen einen Abgleich basierend auf der festen Codierung durch, die für jede einzelne Datei eindeutig ist. Da der Hash einer Datei sehr leicht geändert werden kann, sind Hash-basierte Signaturen nicht sehr effektiv bei der Erkennung polymorpher Malware oder Varianten derselben Datei.

einzuschleusen, weitere Befehle zu geben und Daten zu stehlen. Unser CnC-Schutzmechanismus trennt die unbefugten Kommunikationskanäle und blockiert ausgehende Anfragen zu Domains mit schädlichen Aktivitäten sowie von bekannten, auf infizierten Geräten installierten CnC-Toolkits. Palo Alto Networks lässt die reine Standardautomatisierung von CnC-Signaturen hinter sich, die auf URLs und Domains basiert. Wir erstellen musterbasierte CnC-Signaturen automatisch und liefern so in technikgestützter Geschwindigkeit und Größenordnung CnC-Signaturen auf höchstem Niveau.

Überprüfung auf alle Bedrohungen in einem Durchlauf

Die Threat Prevention-Engine von Palo Alto Networks stellt eine Neuheit in der Branche dar, da sie Datenverkehr untersucht und klassifiziert sowie Malware und Sicherheitslücken-Exploits in einem Durchlauf erkennt und blockiert. Traditionelle Bedrohungsschutztechnologien erfordern zwei oder mehr Scanning-Engines, was zu einer erheblichen Latenz führt und die Durchsatzleistung beträchtlich verlangsamt. Wir nutzen ein einheitliches Signaturformat für alle Bedrohungen, um eine schnelle Verarbeitung zu gewährleisten. So werden alle Analysen in einem einzigen, integrierten Scan durchgeführt, und überflüssige Prozesse, die bei Lösungen mit mehreren Scanning-Engines üblich sind, werden eliminiert.

Unsere Bedrohungsschutztechnologie überprüft jedes Paket im Detail, wenn es die Plattform durchläuft. Bytefolgen sowohl im Paketheader als auch in der Nutzlast werden dabei genau untersucht. Anhand dieser Analysen können wichtige Detailinformationen über das Paket identifiziert werden. Dazu gehören die verwendete Anwendung, Quelle und das Ziel, sowie die Frage, ob es sich um ein RFC-konformes Protokoll handelt und ob die Nutzlast einen Exploit oder Schadcode enthält. Über individuelle Pakete hinaus analysieren wir außerdem den durch die Ankunftsreihenfolge und die Abfolge mehrerer Pakete bereitgestellten Kontext, um Umgehungsmethoden zu erkennen und ihnen vorzubeugen. Die gesamten Analysen und der Signaturenabgleich werden in einem einzigen Scan durchgeführt, sodass der Datenverkehr in Ihrem Netzwerk so schnell bleibt, wie Sie ihn benötigen.

Integration des Bedrohungsschutz-Abonnements mit WildFire

Der WildFire-Service bietet Unternehmen die Möglichkeit, ihre Schutzmechanismen gegen Zero-Day-Malware und Exploits zu erweitern. Bei WildFire handelt es sich um die branchenweit führende Analyse- und Schutzengine für besonders ausgereifte evasive Zero-Day-Malware und Exploits. Bei dem cloudbasierten Service kommt ein einmaliger Ansatz mit mehreren Technologien zum Tragen, bei dem dynamische und statische Analysen, innovative Technologien für maschinelles Lernen sowie eine innovative Bare-Metal-Analyseumgebung miteinander kombiniert werden, um selbst hochgradig evasive Bedrohungen zu ermitteln und verhindern zu können.

Verringern der Angriffsfläche

SSL-Entschlüsselung

Fast 40 Prozent des Netzwerkdatenverkehrs von Unternehmen sind SSL-verschlüsselt, was zu einer großen Lücke in den Schutzvorrichtungen des Netzwerks führt, falls dieser Datenverkehr nicht entschlüsselt und auf Bedrohungen überprüft wird. Unsere Plattform verfügt über eine integrierte SSL-Entschlüsselung, die selektiv zur Entschlüsselung von eingehendem und ausgehendem SSL-Datenverkehr genutzt werden kann. Nachdem der Datenverkehr entschlüsselt und als sicher eingestuft wurde, wird er erneut verschlüsselt und an sein Ziel weitergeleitet.

Blockieren von Dateien

Circa 90 Prozent der schädlichen Dateien, die bei Spear-Phishing-Angriffen zum Einsatz kommen, sind ausführbare Dateien. Bedenkt man außerdem, dass etwa 60 Prozent der Sicherheitszwischenfälle auf Nachlässigkeit von Mitarbeitern zurückzuführen sind, bedeutet dies, dass Ihre Benutzer möglicherweise nicht wissen, was sicher ist und was nicht. Verringern Sie die Wahrscheinlichkeit einer Malware-Infektion, indem Sie gefährliche Dateitypen wie ausführbare Dateien vom Eintritt in Ihr Netzwerk abhalten, die bekanntlich häufig versteckte Malware enthalten. Die Datei-Blockierung kann mit der User-ID kombiniert werden, um basierend auf den Aufgabenbereichen von Benutzern unnötige Dateien zu blockieren. So wird sichergestellt, dass alle Benutzer auf die Dateien Zugriff haben, die sie benötigen, und Ihnen steht eine Möglichkeit zur Verfügung, Risiken granular und auf die Weise zu verringern, die sich aufgrund der verschiedenen Anforderungen in Ihrem Unternehmen anbietet. Reduzieren Sie weiterhin die Anzahl der Angriffsmöglichkeiten, indem Sie alle zugelassenen Dateien zur Analyse an WildFire senden. So kann festgestellt werden, ob sie Zero-Day-Malware enthalten.

Schutz vor unbeabsichtigtem Herunterladen

Ahnungslose Benutzer laden unter Umständen unabsichtlich Malware herunter, indem sie einfach nur ihre Lieblingswebseite besuchen. Oft sind sich der Benutzer und sogar der Betreiber der Website nicht bewusst, dass die Website angegriffen wurde. Wir identifizieren potenziell gefährliche Downloads und senden dem Benutzer eine Warnung, damit sichergestellt ist, dass der Download beabsichtigt erfolgt und zulässig ist. Verhindern Sie Angriffe von neuen und sich schnell ändernden Domains, indem Sie dieses Merkmal mit den URL-Filterungs- und Datei-Blockierungsrichtlinien verknüpfen.

Einfache und präzise Risikominderung

DNS Sinkhole

Unser CnC-Schutz geht einen Schritt weiter und bietet Sinkhole-Funktionen für ausgehende Anfragen an schädliche DNS-Einträge. So kann die Ausschleusung von Daten verhindert und das Opfer präzise identifiziert werden.

Konfigurieren Sie das Sinkhole so, dass alle ausgehenden Anfragen an eine schädliche Domain oder IP-Adresse stattdessen an eine interne IP-Adresse Ihres Netzwerks weitergeleitet werden. Auf diese Weise wird die CnC-Kommunikation effektiv blockiert, und es wird verhindert, dass solche Anfragen überhaupt das Netzwerk verlassen. Es wird ein Bericht zu den Hosts in Ihrem Netzwerk erstellt, die solche Anfragen senden, und das auch dann, wenn diese Hosts sich hinter dem DNS-Server befinden. Die Incident Response-Teams erhalten täglich eine Liste befallener Rechner, bei denen eingegriffen werden muss. Die zusätzliche Belastung während der heißen Phase der Problembehebung fällt weg, da die Kommunikation zum Angreifer bereits abgeschnitten ist.

Automatisierte Korrelationsobjekte

Unsere Bedrohungsschutztechnologie bietet Ihnen die Möglichkeit, die Anwesenheit komplexer Bedrohungen durch die Überwachung und Korrelation von Netzwerkdatenverkehr und Threat-Protokollen zu identifizieren. Auf diese Weise können Sie infizierte Benutzer rasch ermitteln und auffällige Verhaltensmuster analysieren. Die Korrelationsobjekte nutzen die Bedrohungsforschung von Unit 42 sowie die WildFire-Analyse unbekannter Bedrohungen und User-ID, um Zusammenhänge zwischen Anomalien im Datenverkehr und Anzeichen auf eine Gefährdung zu ermitteln. So können die infizierten Geräte in Ihrem Netzwerk schnell und präzise ermittelt werden.

Nutzen Sie unsere globalen Bedrohungsinformationen, um Angriffen vorzubeugen

Detaillierte Protokolle aller Bedrohungen sind nicht nur in derselben Managementoberfläche untergebracht, sie werden auch von allen Schutzereignissen geteilt, um den entsprechenden Kontext zu bieten. Wir nutzen unsere globalen Bedrohungsinformationen via WildFire, um automatisch unbekannte Malware zu entdecken und Schutzfunktionen für unseren gesamten Kundenstamm bereitzustellen. Auf diese Weise können wir den ständigen Schutz unserer Kunden vor den neusten komplexen Bedrohungen gewährleisten.

Passives DNS-Netzwerk

Modell	Gefahrenabwehr-Durchsatz
PA-200	50 Mbit/s
PA-500	100 Mbit/s
PA-2020	200 Mbit/s
PA-2050	500 Mbit/s
PA-3020	1 Gbit/s
PA-3050	2 Gbit/s
PA-3060	2 Gbit/s
PA-5020	2 Gbit/s
PA-5050	5 Gbit/s
PA-5060	10 Gbit/s
PA-7050	100 Gbit/s*
PA-7080	160 Gbit/s*

*aktiviertes DSRI

Schützen Sie Ihr Unternehmen vor sich schnell entwickelnden Malware-Netzwerken und schädlichen Websites, indem Sie die DNS-basierten Analysen von Palo Alto Networks nutzen. Profitieren Sie von einem umfangreichen Informationsnetzwerk und aktivieren Sie die passive DNS-Überwachung, deren Daten unserer Datenbank schädlicher Domains zugeführt werden und die dann verwendet werden, um für unseren weltweiten Kundenstamm wirksame Schutzfunktionen zu generieren.

Unit 42: Bedrohungserforschung

Unit 42, das Palo Alto Networks-Forschungsteam für Bedrohungen, nutzt menschliche Intelligenz, um kritische Zero-Day-Schwachstellen in Microsoft®, Adobe®, Apple®, Android™ und weiteren Systemen zu ermitteln. Wir setzen auf eine proaktive Ermittlung solcher Schwachstellen, Entwicklung von Schutzmechanismen für unsere Kunden und die gemeinsame Nutzung der Informationen mit der gesamten Sicherheitscommunity und nehmen den Angreifern damit die Waffen, die sie einsetzen, um Benutzer zu bedrohen und in die Netzwerke von Unternehmen, Regierungen und Dienstanbietern einzudringen.

4401, Great America Parkway
Santa Clara, CA 95054

Zentrale: +1/408/75 34 000
Vertrieb: +1/866/320/4788
Support: +1/866/89 89 087

www.paloaltonetworks.com