German WildFire Cloud

Vermehrt umgehen hochentwickelte Cyberangriffe durch getarnte und hartnäckige Methoden traditionelle Security-Maßnahmen, wodurch Ihre herkömmlichen Antivirus-, Intrusion Prevention- und zweckgebundenen Sandbox-Appliance-Systeme keinen hochwertigen Schutz mehr leisten können. Die von Palo Alto Networks entwickelte WildFire-Technologie dient, entsprechend den neuartigen Aufgaben, als zusätzliche Schutzmaßnahme zur Verteidigung gegen fortgeschrittene, anhaltende Bedrohungsarten (APTs).

Identifikation von unbekannten Bedrohungen

Die German WildFire Cloud der ICS identifiziert unbekannte Malware, Zero-Day-Attacken und APTs durch Ausführung dieser Bedrohungen in einer skalierbaren, cloud-basierten Sandbox-Umgebung.

Profitieren Sie vom verbesserten Schutz einer cloud-basierten Analyseplattform durch den Zugang zur German WildFire Cloud. Falls in der von Ihrer Firewall nativ klassifizierten Traffic unbekannte bzw. neue PDF-, RTF-, Office-Dokumente und PE-Dateien entdeckt werden, welche EXEs, DLLs, Fonts sowie weitere Typen beinhalten, werden diese zukünftig an die WildFire Systeme der ICS übermittelt. Verdächtiges Verhalten und bösartige Cyber-Angriffe werden dort durch dynamische sowie statische Analyseverfahren in kürzester Zeit aufgedeckt.

Automatischer Schutz durch globale Verteilung

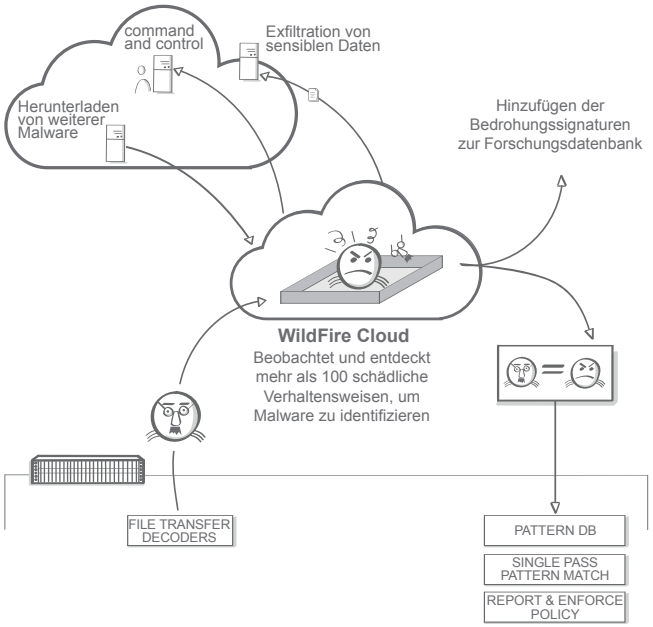
Das Erkennen einer Bedrohung ist der erste Schritt, doch der wahre Wert der WildFire liegt im Schutz jedes einzelnen Benutzers und Netzwerks. Bei Identifikation einer unbekannten Bedrohung generiert WildFire einen automatischen Schutz, um die Bedrohung und die mögliche Ausbreitung zu verhindern. Der generierte Schutz wird dann per Update in maximal 15 Minuten an alle WildFire-Nutzer weltweit verteilt. Durch diese schnelle Schutzverteilung kann die rapide Ausbreitung der Malware und weiterer zukünftiger Variationen ohne zusätzliche Tätigkeit oder Analyse bei allen Nutzern erkannt bzw. blockiert werden.

Des Weiteren werden bekannte Bedrohungen proaktiv über die Threat-Prevention geblockt, welche als erste etablierte Verteidigungsmaßnahme gegen die schon bekannten Malware, Exploits und bösartigen URLs dient.

In Verbindung mit dem Schutz vor schädlichen Dateien oder Exploits bieten wir Ihnen eine tiefgehende Analyse der schädlich abgehenden Kommunikation, störenden Command-and-Control-Aktivitäten mit Anti-C2-Signaturen und den DNS-basierten Callback-Signaturen an. Denn auch diese Informationen fließen zusätzlich in die Palo Alto Networks Datenbanken ein, wo neu entdeckte bösartige URLs automatisch blockiert werden. Diese Korrelation von Daten und In-Line-Schutzmaßnahmen sind der Schlüssel zur Identifizierung sowie Abwehr von Einbruchsversuchen bzw. zukünftigen Angriffen auf Ihr Netzwerk. Nur durch diese kombinierten Maßnahmen können sowohl bekannte als auch unbekannte Bedrohungen frühzeitig entdeckt und verhindert werden.

Vorgehensweise mittels WildFire:

1. Reduzierung der Angriffsfläche durch aktive Sicherheitskontrollen.
2. Blockierung der bekannten Bedrohungen durch dauerhafte Überwachung des Traffics, der Ports und Protokolle.
3. Schnelle Aufdeckung der unbekannten Bedrohungen durch Durchführung und Überwachung der wirklichen Verhaltensweisen von eingehenden, unbekannten Inhalten in der German WildFire Cloud.
4. Automatische Entwicklung neuer Schutzmaßnahmen mit anschließender Integration in die Abwehrmechanismen aller WildFire-Nutzer, wodurch die unbekannten zu bekannten Bedrohungen und somit die Bedrohungen für alle unterbunden werden.



Die Stärke der WildFire Cloud nach deutscher Konformität

Die Lösung ist eine cloud-basierte Architektur, welche für Sie in unseren Rechenzentren betrieben wird. Sie können die German WildFire Cloud ohne zusätzliche Hardwarekosten durch Ihre bestehenden Palo Alto Networks-Firewalls nutzen und erhalten somit den Zugang zu den dynamisch skalierten Malware-Analysen sowie der automatischen Verteilung von Schutzmaßnahmen. WildFire entspricht absichtlich einer sehr genauen Hardwarenachbildung, um realitätsnah verdächtige Proben zu analysieren und auszuführen.

Durch den redundanten Aufbau der Umgebung in zwei deutschen Rechenzentren der DTS-Gruppe garantieren wir Ihnen eine Sicherheitslösung, welche den deutschen Regularien bzw. der Konformität nach dem Bundesdatenschutzgesetz entspricht. Alle verdächtigen Dateien werden sicher sowie verschlüsselt zwischen Ihrer Firewall und einem unserer Rechenzentren übertragen. Nach der Analyse werden gutartige Dateien vernichtet, während schädliche Dateien für weitere Analysen archiviert bzw. sicher aufbewahrt werden. Hierdurch gewähren wir Ihnen die Privatsphäre Ihrer Daten.

ICS bietet als erstes deutsches Unternehmen mit der German WildFire Cloud eine virtuelle Malware-Analyse-Umgebung nach deutschem Recht an. Sie kann über alle Firewalls hinweg gemeinsam verwendet werden, anstatt an jedem Ein-, Ausgangs- und Netzwerkpräsenzpunkt separate Hardware einzusetzen. Dieser Ansatz garantiert Ihnen den maximalen Vorteil aus der gemeinsamen Nutzung von Informationen gegen Bedrohungen mit gleichzeitig minimalen Hardwareanforderungen.

Reporting und Korrelation

Außerdem versorgt WildFire Sie mit integrierten Protokollen, Analysen und Einsichten in WildFire-Ereignisse auf der Administrationsoberfläche von Palo Alto Networks oder Panorama. Dadurch haben Sicherheitsexperten die Möglichkeit, die im Netzwerk beobachteten Ereignisse umgehend zu untersuchen und zu korrelieren. Somit können Sie die Daten, welche Sie für frühzeitige Untersuchungen und Reaktionsmaßnahmen auf Vorfälle benötigen, schnell lokalisieren sowie anschließend in Aktionen wie Protokollanfragen oder benutzerdefinierte Signaturen umsetzen.

Diese Informationen liefern wichtige Erkenntnisse über schädliches Verhalten, z.B. über sondierte Domains, erstellte Dateien und betroffene Registrierungseinträge.

Zur Unterstützung der Security und zur Aufdeckung von infizierten Hosts bietet WildFire auch:

- Ausführliche Analysen zu jeder böswilligen, an WildFire gesandten Datei einschließlich sowohl client- als auch netzbasierte Tätigkeiten
- Sitzungsdaten, welche mit der böswilligen Malware in Verbindung stehen, einschließlich Quelle, Bestimmungsort, Anwendung, User-ID™, URL-Adresse, usw.
- Zugang z. B. zu originalen Malwaresamples zwecks Rekonstruktion bzw. Nachbildung und zu allen PCAPs aus den dynamischen Analyse-Sessions
- Eine Analyse liefert viele Gefährdungshinweise, durch die gezielt gegen die ganze APT-Kill-Chain vorgegangen werden kann