Blue Shield Umbrella: Technische Beschreibung

Der Blue Shield Umbrella ist ein Cloud-basiertes DNS-System, das Gefahren bereits abwehrt, bevor sie in das LAN des Kunden gelangen können. Es überwacht den laufenden DNS-Verkehr und entscheidet in Echtzeit anhand von diversen mathematischen Algorithmen, ob Anfragen erlaubt werden oder nicht. Auf diese Weise werden unbekannte Angriffe unterbunden. Der prinzipielle Unterschied zu konventionellen Systemen ist, dass keine Signaturen und Ähnliches zum Einsatz kommen, sondern künstliche Intelligenz.
Zum Beispiel: Predictive und evolutionäre Algorithmen und zahlreiche weitere hochspezifische mathematische Algorithmen zur Bewertung von Domains. Auf einer sogenannten „WhiteList" Root Nameserver Basis wird schon vorsortiert, bevor eine Domain in unser DNS-System aufgenommen wird. Zu dieser Bewertung, ob eine Domain auf der Blue Shield Umbrella-Plattform aufgenommen wird, kommen speziell entwickelte Sandbox-Lösungen von verschiedenen Herstellern, eigene Crawler und ein ganz neuartiger Algorithmus zum Einsatz, welcher jeglichen Web Code auf schadhafte Software scannen und auch weiterführende Links prüfen kann, z.B. für CDN Networks, Forum Links usw. - dadurch setzen wir im Bereich ZeroDay Prävention neue Maßstäbe. Zudem forschen und entwickeln wir im Bereich Command and Control Traffic weit über den bekannten DGA (Domain Generation Algorithm) hinaus, da Blue Shield Umbrella den unbekannten C&C Traffic blockiert, wo IPS-Systeme und Reputation Services durch ihre Architektur versagen.

Mit insgesamt 20 Entwicklern im Haus und internationalen universitären Kooperationen entwickeln wir aktiv unsere Threat Intelligence im Bereich ZeroDay, C&C und vielen anderen Bereichen weiter.

Des Weiteren kooperieren wir aktuell mit 15 namhaften Herstellern, sodass ein sekündlicher Datenaustausch passiert, um die Treffsicherheit zu gewährleisten und einen False Positive (statische Fehlentscheidung) zu vermeiden.

Bei der sogenannten Real Time Prevention werden keine Ergebnisse gespeichert, sondern bei jedem Aufruf in Echtzeit die Verbindungsdaten des Zieles geprüft und mit Algorithmen unter Verwendung historischer Daten bewertet, ob das aktuelle Verhalten gut oder schlecht ist. Sollte sich eine Infrastruktur drastisch ändern, sodass die historischen Daten nicht mehr zum aktuellen Verhalten passen, sperren wir die Domain bis zur neuen Erstellung eines Profils für die Real Time Prevention.

Parallel laufen für die aufgerufenen Hosts im Hintergrund Code Scans auf Basis des neuen mathematischen Algorithmus inklusive der speziell entwickelten Sandbox, um auch neben den Verbindungsdaten sofort zu erkennen, wenn sich ein Code bösartig verändert. Diese Information wird laufend herangezogen um festzustellen, ob die gewünschte Domain auf unseren Klonen der Root Nameserver weiterhin anerkannt wird.