Mit AlienVault die Spuren von Cyberkriminellen verfolgen

Mit AlienVault die Spuren von Cyberkriminellen verfolgen

Verdächtige Domains mit Hilfe von DNS-Protokollen identifizieren
München/San Mateo, 22. Oktober 2013 - Die Taten von Cyberkriminellen nachzuverfolgen, ist ein schwieriges Unterfangen. Doch wenn die Internet-räuber eine neue Infrastruktur angreifen, weisen ihre für die Attacke genutzten Domain-Namen oft auf temporäre Adressen hin. Dies sind zumeist DNS (Domain Name System)-Server und andere Infrastrukturen großer Internetunternehmen wie z.B. Google. Unified Security Management (USM)-Anbieter AlienVault verrät effektive Techniken, mit denen Firmen verdächtige Domains via DNS-Logging (Protokollierung) aufspüren können.
Ein zum DNS-Logging verwendetes Tool ist PassiveDNS. Es ermöglicht Nutzern, den DNS-Traffic eines Interfaces sichtbar zu machen. Zudem kann die Lösung DNS-Anfragen in einer MySQL-Datenbank für weitere Abfragen und Analysen speichern. Um den Verkehr der DNS-Server aufzuarbeiten, rät AlienVault dazu, einen Span- oder Mirror-Port auf dem Router/Switch zu aktivieren. Für diesen Prozess stellt der USM-Anbieter einige Tutorials als Anleitung bereit.
Sobald Nutzer in der Lage sind, den Verkehr der DNS-Server auszulesen, oder wenn der Fall eintritt, dass interne Systeme mit externen DNS-Servern kommunizieren, sind Konfigurationen an PassiveDNS nötig. Nachdem alles eingerichtet ist, beginnt die Lösung, DNS-Anfragen von internen Systemen zu sammeln und zu speichern. Anwender können sämtliche Informationen nun über das Web-Interface von PassiveDNS abfragen. Dadurch sind sie in der Lage, Vorgänge mit verdächtigen Domains zu identifizieren und die bösartigen auszufiltern.
Intrusion Detection mit Suricata
Eine zweite Lösung zum Aufspüren verdächtiger Domains basiert auf einer Beta-Version des in OSSIM und AlienVault USM integrierten Netzwerk-Intrusion Detection-Systems (IDS) Suricata. Suricata beinhaltet ein Modul, das DNS-Anfragen und -Antworten protokolliert. Nach dem Download von Suricata-20beta1 überblicken Anwender in einer Datei den Netzwerkverkehr in Form von DNS-Protokollen. Danach werden die AlienVault-Lösungen so konfiguriert, dass sie die zuvor ausgelesenen Daten sammeln. Das Unternehmen stellt zum Test ein Beta-Plugin dieser Lösung unter https://github.com/AlienVault-Labs/AlienVaultLabs/tree/master/plugins bereit.
Im Anschluss verarbeitet OSSIM die Ausgaben des Suricata DNS-Moduls. In der AlienVault USM-Web-Oberfläche können Nutzer nun gezielt nach Domains mit gewissen Kriterien suchen. Der Vorteil dieser Konsole ist, dass die IP-Adresse der Maschine, von der die DNS-Anfrage kommt, mitgeteilt wird. Zudem erhalten Anwender weitere Informationen über verbundene Systeme in der gleichen Konsole, beispielsweise zu NetFlow-Daten, IDS-Daten, Inventardaten, Schwachstellen, Sicherheits-Events von anderen Geräten etc. Dank der Integration der Konsole und der Möglichkeit, alle relevanten Daten durch ein Fenster zu betrachten, wird die forensische Untersuchung kompromittierter Systeme wesentlich einfacher.

Über AlienVault:
Die Unified Security ManagementTM-Plattform AV-USM von AlienVault bietet Unternehmen mit eingeschränktem Security-Personal und Budget einen schnellen und kostengünstigen Weg, die Anforderungen an Compliance und Threat Management zu erfüllen. Da alle essenziellen Kontrollfunktionen bereits integriert sind, fungiert AV-USM als Security-Umgebung der Enterprise-Klasse, auch für kleine Security-Teams, die mit weniger mehr erreichen wollen. AlienVaults Open Threat ExchangeTM ist ein offenes und kollaboratives System für die Kommunikation unter Security-Spezialisten (auch mit Kunden) im Bereich Threat Intelligence und somit eine Art Lernplattform mit Experten und Researchern, die sich über die neuesten Bedrohungen und Verteidigungstaktiken austauschen. AlienVault ist ein Privatunternehmen mit Hauptsitz in Silicon Valley (Kalifornien/USA) und wird von Kleiner Perkins Caufield
 Byers, Sigma, Trident Capital und Adara Venture Partners unterstützt. Die Märkte in Deutschland, Österreich und der Schweiz werden von der AlienVault Deutschland GmbH mit Sitz in Ismaning betreut. Für weitere Informationen besuchen Sie www.alienvault.de oder folgen Sie uns auf Twitter.

Weitere Informationen:
AlienVault Deutschland GmbH
Gutenbergstraße 6
D-85737 Ismaning
 www.alienvault.com
Ansprechpartner:
Alexander Goller
Solutions Architect
Tel.: +49 (0) 89-12 76 68 65
Fax: +49 (0) 89-97 89 93 42
E-Mail: agoller@alienvault.com
PR-Agentur:
Sprengel
 Partner GmbH
Nisterstraße 3
D-56472 Nisterau
 www.sprengel-pr.com
Ansprechpartner:
Fabian Sprengel
Tel.: +49 (0) 26 61-91 26 0-0
Fax: +49 (0)26 61-91 26 0-29
E-Mail: alienvault@sprengel-pr.com
<img src="http://www.pressrelations.de/new/pmcounter.cfm?n_pinr_=548088" width="1" height="1">

Pressekontakt

AlienVault Deutschland GmbH

85737 Ismaning

agoller@alienvault.com

Firmenkontakt

AlienVault Deutschland GmbH

85737 Ismaning

agoller@alienvault.com

Über AlienVault:Die Unified Security ManagementTM-Plattform AV-USM von AlienVault bietet Unternehmen mit eingeschränktem Security-Personal und Budget einen schnellen und kostengünstigen Weg, die Anforderungen an Compliance und Threat Management zu erfüllen. Da alle essenziellen Kontroll-funktionen bereits integriert sind, fungiert AV-USM als Security-Umgebung der Enterprise-Klasse, auch für kleine Security-Teams, die mit weniger mehr erreichen wollen. AlienVaults Open Threat ExchangeTM ist ein offenes und kollaboratives System für die Kommunikation unter Security-Spezialisten (auch mit Kunden) im Bereich Threat Intelligence und somit eine Art Lernplattform mit Experten und Researchern, die sich über die neuesten Bedrohungen und Verteidigungstaktiken austauschen. AlienVault ist ein Privatunternehmen mit Hauptsitz in Silicon Valley (Kalifornien/USA) und wird von Kleiner Perkins Caufield & Byers, Sigma, Trident Capital und Adara Venture Partners unterstützt. Die Märkte in Deutschland, Österreich und der Schweiz werden von der AlienVault Deutschland GmbH mit Sitz in Ismaning betreut. Für weitere Informationen besuchen Sie www.alienvault.de oder folgen Sie uns auf Twitter.