FIREEYE™

LÖSUNGSÜBERSICHT

Intelligenter Serverschutz

Neue Funktionen in Network Security und Endpoint Security zur Abwehr komplexer Angriffe

HIGHLIGHTS

- Versierte Hacker greifen Server mit Methoden an, die nur schwer entdeckt werden können.
- FireEye bekämpft die Bedrohung sowohl im Netzwerk als auch auf dem Server.
- Dank Bedrohungsdaten können FireEye-Lösungen auch Angriffe aufdecken, die anderen Anbietern verborgen bleiben.

Überblick

Heutzutage werden Geschäfte häufig außerhalb der Unternehmen abgeschlossen und die meisten Angestellten arbeiten auf Mobilgeräten, die fortlaufend Daten mit Servern in Rechenzentren und in der Cloud austauschen. Dadurch wird jedoch ein Angriffspfad zu den wichtigsten Vermögenswerten des Unternehmens offengelegt, die auf den Servern gespeichert sind: Daten, Kundeninformationen und geistiges Eigentum.

Auf den Servern werden häufig Webanwendungen ausgeführt, die sowohl über das Internet als auch im jeweiligen Unternehmen zugänglich sind. Hacker können einen Server direkt von außen angreifen. Dazu durchleuchten sie ihn, um festzustellen, welches Betriebssystem und welche Webservices und -anwendungen ausgeführt werden, und wählen dann Sicherheitslücken oder Exploits für ihren Angriff aus.

Die Sicherheitsbranche bietet zahlreiche Lösungen zum Schutz von Endpunkten und Netzwerken, aber Server – sowohl mit Linux als auch Windows – haben andere Angriffsflächen, Sicherheitslücken und Muster als Endpunkte. Hacker agieren auf den Servern im Verborgenen und bleiben im Durchschnitt sogar 78 Tage lang unentdeckt. So haben sie viel Zeit, sich umzusehen, Berechtigungen auszuweiten, die vertraulichsten Daten eines Unternehmens zu stehlen und anschließend ihre Spuren zu verwischen.

Methoden für Angriffe auf Server

Ein Angriff auf einen Server unterscheidet sich in der Regel erheblich von einem Angriff auf einen Endpunkt. Der Hacker möchte sich möglichst lange im System aufhalten, um Daten aus dem Netzwerk, personenbezogene Daten oder Informationen zu Finanztransaktionen zu sammeln. Je länger er unerkannt bleibt, desto mehr wertvolle Informationen kann er stehlen. Einfache Angriffsmethoden wie Malware oder Würmer können schnell abgewehrt werden. Versierte Hacker nutzen Webshells als Trojaner für den Fernzugriff und schreiben einige Codezeilen auf den Webserver, um eine Backdoor zu installieren oder sich Zugriff auf das Dateisystem des Servers zu verschaffen.

Diese Zeilen ähneln dem Code, der bereits auf dem Server vorhanden ist. Solange die Webshell nicht aktiv ist, ist sie daher nur sehr schwer zu finden. Mithilfe von Webshells können Hacker Suchmaschinenanfragen auf eine manipulierte Webseite umleiten oder auch der Suchmaschine andere Inhalte präsentieren als dem Benutzer. Um eine Webshell zu finden, muss in der Regel der User-Agent des Webcrawlers geändert werden.

Methoden zur Erkennung von Angriffen
Automatisierte Tools können in der Regel keine Webshell-Angriffe erkennen. Administratoren müssen sich daher auf die folgenden Indikatoren verlassen, um solche Angriffe aufzudecken:

- Ungewöhnlich hohe Webserverauslastung (aufgrund der Uploads und Downloads der Hacker)
- Dateien mit einem ungewöhnlichen Zeitstempel (z. B. einem neueren Datum als das der letzten Änderung)
- Unbekannte Dateien auf dem Server
- Dateien mit zweifelhaften Referenzen, wie cmd.exe oder eval-Funktionen
- Unbekannte Verbindungen in den Logdateien des Webservers

Experten können zwar die Logdateien des Webservers analysieren, um den Speicherort der Webshell zu finden, aber diese Arbeit ist sehr zeitaufwendig, da alle verdächtigen Logdateien überprüft werden müssen. Und währenddessen ist der Hacker weiterhin im System aktiv.

Herkömmliche Sicherheitstools können gegen fortschrittliche Serverangriffe wenig ausrichten. Firewalls und Intrusion-Detection-Systeme basieren in der Regel auf Signaturen, die jedoch von Webshells recht einfach umgangen werden können. Secure Web Gateways und andere Produkte analysieren eventuell den Inhalt, aber da in Webshells legitimer Code verwendet wird, werden sie bei diesen Prüfungen nicht erfasst. Unternehmen benötigen eine Lösung, mit der sie das gesamte System nachbilden, mit Code interagieren und nach Indikatoren suchen können, um anschließend zu überprüfen, ob es sich um Schadcode handelt.

Die Lösungen von FireEye
Die neuen Funktionen in FireEye Network Security und Endpoint Security erkennen Webshell-Datenverkehr, überprüfen, ob ein Server infiziert wurde, und ermöglichen eine genauere Untersuchung, um den Angriff abzuwehren.

Network Security
Mit der FireEye SmartVision-Engine in Network Security können Kunden den Netzwerkverkehr überprüfen und schädlichen Datenverkehr zwischen den Clients und den Netzwerkgeräten erfassen, die über SMB kommunizieren. FireEye Network Security 8.3 kann Webshell-Datenverkehr erkennen, die Aktivitäten der Webshell nachverfolgen und feststellen, wann sie aktiv ist und welche Geräte verwendet werden. Anhand dieser Informationen können Incident-Response-Teams akute Angriffe erkennen und die notwendige Untersuchung einleiten.

Endpoint Security
FireEye Endpoint Security verwendet vier spezielle Engines, um Microsoft Windows-Clients und Windows-Server zu schützen sowie Angriffe zu erkennen und abzuwehren. Auf Linux-Servern können Incident-Response-Teams die Echtzeiterkennungs- und Untersuchungsfunktionen von Endpoint Security 4.8 nutzen.

Mit diesen beiden aktualisierten Lösungen können Experten zuerst mit Network Security überprüfen, ob die Webshell bei einem Serverangriff eingesetzt wird und welche Server betroffen sind. Anschließend untersuchen sie mit Endpoint Security diese Server genauer und ermitteln, welche Webseiten oder -anwendungen mit der Webshell manipuliert wurden. Im nächsten Schritt werden diese Webseiten oder -anwendungen isoliert und die Fehler in der Umgebung behoben, damit der reguläre Betrieb wieder aufgenommen werden kann. Wenn sie wissen, wie der Angriff durchgeführt wurde, können Sicherheitsteams weitere Infektionen verhindern, indem die Sicherheitslücken behoben oder die betroffenen Systeme gepatcht werden. Eine ähnlich proaktive Fehlerbehebung lässt sich auch als Präventionsmaßnahme auf den übrigen Servern anwenden.

Zusammen besser
Mit diesem Sicherheitspaket von FireEye dauert es nicht mehr Wochen, bis Angriffe erkannt und abgewehrt werden, sondern nur noch wenige Stunden. Infizierte Dateien oder Anwendungen können sogar innerhalb von Minuten behoben werden, statt wie bisher erst nach mehreren Tagen. FireEye stellt seinen Kunden ein umfassendes Produktpaket für den Lebenszyklus von der Erkennung bis zur Untersuchung zur Verfügung. Damit können auch tiefgreifende Angriffe in Rechenzentren abgewehrt werden, die kaum ein anderer Anbieter erfasst.

Mehr Informationen zu FireEye erhalten Sie unter: **www.FireEye.de**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035, USA
+1 408 321 6300/+1 877-FIREEYE (347 3393)/
info-dach@FireEye.com

Über FireEye, Inc.
FireEye spezialisiert sich auf datengestützte Sicherheit. FireEye erweitert die Sicherheitskapazitäten seiner Kunden nahtlos und skalierbar und bietet über eine einheitliche Plattform die weltweit anerkannten Beratungsdienste von Mandiant®, innovative Sicherheitstechnologien und Bedrohungsdaten an, die denen staatlicher Sicherheitsbehörden in nichts nachstehen. Mit diesem Ansatz übernimmt FireEye die Verantwortung für die Vorbereitung von Kundenunternehmen auf die Erkennung und Abwehr von Cyberangriffen.

FIREEYE™