Embedded-Systeme vor zielgerichteten Angriffen schützen

Hypervisor-Software befriedigt Schutzbedürfnis

Je näher die Vision Internet of Things (IoT) ihrer Verwirklichung kommt, desto dringlicher werden geeignete Maßnahmen zum Schutz der IoT-Infrastruktur und ihrer Kernelemente, der Embedded-Systeme. Herkömmliche Anti-Malware- und Anti-APT-Lösungen (Advanced Persistent Threats) haben der Bedrohung nicht genug entgegenzusetzen. Einen Ausweg können »Bare-Metal«-Hypervisors wie »LynxSecure« von Lynx Software Technologies weisen.

Von Avishai Ziv, Vice President of Cyber Security Solutions bei Lynx Software Technologies

Mit 15 Milliarden Connected Devices – erwartet für 2015 – nimmt das IoT Gestalt an, aber die Zweifel an der Sicherheit der IoT-Infrastruktur werden zugleich immer größer. Spektakuläre gezielte Angriffe über verbundene Objekte zeigen immer wieder eines: Während die Notwendigkeit eines Schutzes vor gewöhnlichen Malware-Angriffen kaum bezweifelt wird, reicht das Bewusstsein für einen adäquaten Umgang mit direkten und zielgerichteten Angriffen auf bestimmte Elemente der Infrastruktur und für damit verbundene spezielle Herausforderungen bei weitem noch nicht aus.

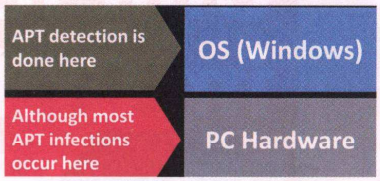
Falls verbundene Embedded-Objekte dieselben Betriebssysteme verwenden wie die IT-Endpunkte, kann diese Embedded-Infrastruktur mittels erprobter Techniken angegriffen werden. Dies ist besonders besorgniserregend, wenn verbundene Embedded-Objekte zur Steuerung strategischer Infrastrukturen wie etwa des öffentlichen Stromnetzes genutzt werden und dadurch zum attraktiven Ziel sowohl für einzelne Hacker als auch für ausländische Regierungen werden.

Die Unternehmens-IT befasst sich schon seit einiger Zeit mit diesem Problem – bislang mit bescheidenem Erfolg. Zwar werden unablässig neue Lösungen zur Bekämpfung ausgefeilter bösartiger APT-Programmcodes vorgestellt. Doch bleibt die Detektionslücke alarmierend groß. Der Hauptgrund: Gängige Sicherheitslösungen können einen tatsächlichen APT-Befall nicht erkennen. Stattdessen konzentrieren sie sich mithilfe herkömmlicher Anti-Malware-Techniken auf gescheiterte Verhinderungsversuche und auf die Beobachtung bereits infizierter Angriffsziele.

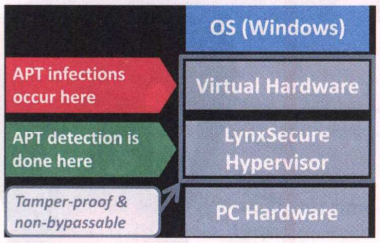
Wie lassen sich solche Angriffe in der Embedded-Welt effektiv erkennen und abwenden? Neue unkonventionelle Erkennungsmethoden lösen das Problem – speziell: ein sicherer Embedded-Hypervisor. Anbieter von Sicherheitsprodukten reagieren auf neue APT-Infektionsmethoden und Techniken, sich der Erkennung zu entziehen, schneller als je zuvor. Dennoch beträgt die durchschnittliche Aufdeckungszeit bei APT immer noch Monate.Hauptursache für die große Detektionslücke (d.h. die Zeit zwischen der ersten Infektion durch einen APT und dem Zeitpunkt seiner Erkennung) sind die ausgefeilten Infektionstechniken der Angreifer. Die meisten Infektionen erfolgen unterhalb des infizierten Betriebssystems und lassen sich daher nicht in Echtzeit mittels herkömmlicher Detektionstechniken aufspüren.

Die wesentlichen Phasen eines APT-Angriffs

Die »Vorbereitungsphasen« (Erkundung, Zielidentifizierung, Einholung der Benutzerkontakte etc.) ebnen den Weg. Doch der eigentliche Angriff beginnt erst, wenn das APT das beabsichtigte Ziel – in der Regel ein Endpunkt – erreicht.



Die APT-Detektionslücke



Wie APT-Erkennung erfolgen sollte

Der APT-Angriff selbst setzt sich aus drei Phasen zusammen:

Eindringen: Ausnutzung von Schwachstellen im Betriebssystem und/oder in der Anwendung, um das eigentliche APT auf dem Endpunkt installieren zu können. Im Embedded-Bereich ist das eine gravierende Schwachstelle, weil Embedded-Endpunkte typischerweise unter veralteten Betriebssystemen wie Windows XP laufen, die nicht länger mit aktuellen Sicherheits-Patches unterstützt werden. Diese ATM- und POS-Terminals sind viel gefährdeter als gewöhnliche PCs.

Infizieren: Installation des eigentlichen APT, üblicherweise als »Dropping« (»Abwurf«) bezeichnet; die APT-Komponente selbst, meist mit einem Rootkit-Modul, wird als »Payload« (»Sprengladung«) bezeichnet. Dies ist DAS kritische Stadium, in dem das Angriffsziel befallen wird: Das APT gewinnt genug Kontrolle über das Zielsystem, um die böswillige Aktivität frei auszuführen.

APT-Aktivität: Die beabsichtigte böswillige Aktivität auf dem infizierten Zielsystem (Kommunikation mit dem C&C-Server, Sammeln persönlicher Informationen, Datenlöschung, Löschung des MBR, Verwandlung des Computers in einen Zombie usw.) wird ausgeführt.

Die klaffende Lücke bei der APT-Erkennung

APTs lassen sich derzeit auf zwei Arten erkennen: Zum einen versuchen Anti-Malware-Lösungen, das Eindringen zu erkennen und zu verhindern (Phase 1) im Kontext ihres Host-Betriebssystems Windows. Zum anderen konzentrieren Anti-APT-Lösungen ihre Detektion auf die tatsächliche Aktivität des APT im bereits infizierten System (Phase 3) durch das Feststellen und Beobachten der Netzwerkaktivität des APT. Die APT-Lösungen verhindern aber weder die Infizierung, noch können sie die Infektion bereits vor der Netzwerkaktivität erkennen.

Es existiert keine Lösung, die den eigentlichen APT-Infizierungsvorgang erkennt – die gefährlichste und ausschlaggebende Angriffsphase – und deshalb exakt zum Zeitpunkt des Geschehens Alarm schlagen kann. Daher die APT-Detektionslücke.

Die meisten APT nutzen Low-Level- und Sub-OS-Rootkits, die eigens dafür entwickelt sind, vom Betriebssystem bzw. von jeder darin oder darauf installierten Sicherheitsanwendung nicht auffindbar zu sein (daher das P für »persistent«, »andauernd«). Um unauffindbar zu sein und dennoch ausreichende Kontrolle über lebenswichtige Funktionen des infizierten Betriebssystems zu erlangen, braucht ein Rootkit typischerweise zwei Dinge: Erstens muss es sich selbst in verborgenen Teilen der Festplatte installieren können, auf die das Betriebssystem nicht zugreifen kann (die unpartitionierten Sektoren zwischen den Festplattenpartitionen und der letzte Sektor der Platte). Zweitens benötigt es Sicherheitsrechte, die dem infizierten Betriebssystem übergeordnet sind (Untergrabung der OS-Bootsequenz, Selbststart vor dem OS durch Abänderung der ursprünglichen OS-Bootsektoren MBR, VBR und UEFI).

Diese zwei Grundmerkmale von Rootkits sind tödlich effektiv: Weil die zum Eindringen in das Betriebssystem verwendeten Dateiinfektoren häufig polymorph sind, verändern sich Rootkits viel langsamer. Neue Versionen tauchen alle 12 bis 18 Monate einmal auf. Da sie so verborgen und unauffindbar sind, besteht wenig Anlass für Veränderungen.

Sub-OS-Erkennung von Sub-OS-Bedrohungen

Nötig ist daher eine neue Herangehensweise, die zwei kritische Aufgaben erledigt: erstens die Erkennung der eigentlichen APT-Infektion in Echtzeit, zweitens die sofortige Versorgung der Bedrohungsabwehr-Beauftragten mit forensischen Daten, um deren Analyse- und Reaktionszeiten signifikant zu verkürzen. Die Erkennung muss, weil APT schwer zu erfassen sind und heimlich vorgehen, auf einer Ebene erfolgen, die unter der der Infektion und Aktivität liegt. Diese Ebene kann nur ein »Bare-Metal«-Hypervisor wie etwa »LynxSecure« sein, der Hardware von Software trennt, aber dem installierten Betriebssystem nur blanke virtuelle Hardware anzeigt. Als letztlich »virtuelles Motherboard« ist solch ein Hypervisor unsichtbar für APT und von ihnen nicht auffindbar.

Der Hypervisor muss speziell für die Erkennung ausgelegt (d.h. ein Honeypot) und so rigoros abgehärtet sein, dass er nicht selbst Angriffsziel wird. Dies hebt auch jegliche Abhängigkeit von OS auf, so dass die Erkennung eine OS-agnostische wird. Als privilegiertester Beobachter auf der Plattform kann der Hypervisor jede Veränderung an der beobachteten Hardware erfassen.

Überdies lässt sich ein gut durchdachter Embedded-Hypervisor mit besonders kleiner eigensicherer Code-Basis in typischen PC-gestützten Embedded-Systemen installieren, die über eher bescheidene Rechenleistung und Speichergröße verfügen. Die geringe Größe des Hypervisors wird das Sicherheitsniveau des Gesamtsystems weiter stärken und die Angriffsoberfläche erheblich reduzieren. Auf diese Weise werden heimlich vorgehende Rootkits sofort abgefangen: MBR-Wiper (z.B. Dark Seoul), MBR-Infektoren (z.B. TLD4), VBR-Infektoren (z.B. XPAJ) oder Malware, die verborgene Dateisysteme nutzt (z.B. ZeroAccess).

Detaillierte und konzentrierte Sicht auf die Hardware

Die Ermittlung der genauen Einzelheiten solcher Infektionen erfordert derzeit eine mühsame und langwierige forensische Analyse. Die forensischen Daten der uninfizierten Hardware sind nicht verfügbar, daher muss die gesamte Hardware auf Infektion hin analysiert werden. Das bedeutet wahrlich die Nadel im Heuhaufen suchen.

Der Hypervisor jedoch erlaubt die Erstellung eines sofortigen und abgestimmten forensischen Berichts, der nur die infizierten Bereiche enthält, zusammen mit einer automatischen Analyse des infizierten Zustands gegenüber dem »sauberen«. Denn ein Hypervisor behält immer das »Gold Image«, also ein sauberes, uninfiziertes Master-Bild.

Zur erfolgreichen Eindämmung von APT-Angriffen ist also ein »Out-of-the-Box«-Ansatz erforderlich. Im Gegensatz zum fertigen, geschlossenen Abwehrsystem kann der Anwender dessen Funktionen frei definieren. Ein sicherer Embedded-Hypervisor zieht die Sicherheit – um im Bild zu bleiben – aus der Box heraus und zu sich selbst als proaktive Erkennungsebene. (ak) ■