APPGUARD

Die Malware-Defensive

Verteidigungsministerium - Gesundheitspflege
Behörde fügt Zero-Day-Server hinzu Verteidigung mit AppGuard

FALLSTUDIE: VERTEIDIGUNGSMINISTERIUM - GESUNDHEITSPFLEGE

HERAUSFORDERUNGEN:

- Schutz vor Zero-Day- und neu gestalteten Malware-Angriffen auf Server mit missionskritischen Anwendungen, bevor erkennungsorientierte Tools und das Personal reagieren können.
- Eliminieren von langen Ausfallzeiten der Infrastruktur aufgrund von Sicherheitsvorfällen, zu denen es trotz erheblicher Investitionen in Ressourcen und Technik kam.

ERGEBNISSE:

- Optimierung von Sicherheitstools und Ressourcen.
- Einfache Bereitstellung, schnelle Amortisierung.
- Mehr Sicherheit, weniger Aufwand.
- Abgehärtete Server, die Angriffe in Echtzeit neutralisieren, was die Störfallüberwachung insgesamt sowie die Anzahl der Vorfallsreaktionen drastisch verkürzt.

Über die Behörde

Die Behörde verwaltet kritische Daten der Gesundheitspflege und Aktivitäten in Bezug auf das US Verteidigungsministerium (U.S. Department of Defense, DoD). In einem solchen kritischen Umfeld sind Sicherheitsbelange entscheidend, um Menschenleben zu schützen.

Situation:

Die Behörde musste zusätzlichen Schutz sowie verbesserte Störfallreaktionszeiten sicherstellen, als sie ihre kritische Infrastruktur auf die Cloud verlegte.
Der vorhandene Ansatz, der HBSS und Carbon Black beinhaltete, bot sowohl Einsicht in die Server-Umgebung als auch einen Ansatz basierend auf Erkennung und Reaktion, um Kompromittierungen zu eliminieren. Jedoch wurden die Server nicht in Echtzeit ohne signifikante falsche Positive geschützt. Hostbasierte Anti-Virus- und Verhaltensanalysetools sind nur erfolgreich, wenn sie Malware oder ihre Auswirkungen erkennen. Angreifer verändern ihre Taktiken, Techniken und Vorgehensweisen, um nicht entdeckt zu werden. Daher erfordert die effektive Nutzung von Lösungen, die auf Erkennung und Reaktion basieren, menschliche Intervention. Dadurch können sich die Reaktionszeiten von Millisekunden auf Minuten oder sogar Stunden erhöhen. Jedoch sind die Auswirkungen umso größer und die Störfallkosten umso höher, je länger die Verzögerung dauert. Bei einer Organisation der Gesundheitspflege in der DoD-Gemeinde können Operationen betreffende Sicherheitsvorfälle Menschenleben in Gefahr bringen.

Diese Server wurden durch ein HBSS und Carbon Black geschützt. Ein HBSS wendet an den Endpunkten Regeln für das Zulassen/Ablehnen an, die Malware-Angriffe abwehren können, ohne sie oder ihre Auswirkungen erkennen zu müssen. Trotzdem machen Änderungen bei Hosts und Widersachern das Ausarbeiten und Pflegen von Regeln schwierig und hinterlassen potenzielle Sicherheitslücken. Obwohl die Erkennung mit Carbon Black beim Blockieren bekannter

Malware und bestimmter Verhaltensweisen effektiv ist, bleibt immer noch Raum für Verbesserungen bei der Störfallreaktionszeit insgesamt.

Lösung: Echtzeitschutz ohne Erkennung; Hostbasierte Software

Die Cybersecurity-Gemeinde hat in den letzten zwei Jahren zunehmend erklärt, dass Unternehmen und Verkäufer, die ihnen Tools anbieten, mehr tun müssen, um die Endpunkte abzuhärten, die von Angreifern attackiert werden. Durch Abhärtung wird Alarmen vorgebeugt, die überwacht und untersucht werden müssen, um abzuwehrende Kompromittierungen zu verhindern. So werden die Arbeitskosten effektiv gesenkt, während der Schutz erhöht wird. Arbeitsaufwand ist der größte einzelne Kostenfaktur im Bereich Cybersecurity.

Das lässt sich nicht mit Perimetertools erreichen. Es muss aus dem Inneren der Server heraus geschehen und auch, wenn es dafür schon immer eine Vielzahl von Methoden gab, sind die traditionellen Optionen mühevoll.

Herkömmliche Abhärtungskontrollen erfordern extreme Detailtreue bei den Anwendungen auf einem Server und auch beim Host selbst. Ungenaue, unvollständige Regelwerke unterbrechen Betriebsabläufe. Das Beschaffen dieser genauen Details und das Implementieren entsprechender Regelwerke waren immer schon sehr schwierig. Das zweite Hindernis sind die Veränderungen. Anwendungen und ihre Hosts verändern sich häufig aufgrund von Updates der Funktionen, Sicherheitspatches, Plugin-Zugängen und mehr. Mit ihnen müssen sich auch die Regeln ändern. Die Häufigkeit notwendiger Änderungen machte das Abhärten über Regelkontrollen bezüglich Bereitstellung und Pflege im Laufe der Zeit unzumutbar beschwerlich. Es wurde eine Lösung für eine Regelwerk-Engine benötigt, die sich automatisch an Updates anpasst - also AppGuard.

AppGuard: Besserer Schutz, weniger Aufwand

Wenn sich noch weitere Endpunkt-Sicherheitsagenten auf den Servern befinden, ist der leichte Fußabdruck von AppGuard bei CPU, Speicher, Laufwerk und Bandbreite wesentlich, um Auswirkungen auf die Leistung des Servers zu verhindern. Der Erfolg von AppGuard liegt in der Abwehr von Angriffen, die zuvor nicht von Tools entdeckt worden wären, die auf vorheriges Verhalten zurückgreifen, um potentielle Angriffe festzustellen. AppGuard ist darüber hinaus effektiver gegenüber neuen Variationen von Angriffen, denn seine Abwehr basiert nicht auf zuvor bestehenden Angriffsmustern.

Funktional passt sich AppGuard automatisch an die normalen Änderungen im Lebenszyklus an, wie Funktionsupdates, Patches und andere Veränderungen der Umgebung, ohne dass die Regelwerke aktualisiert werden müssen. Im Gegensatz zu anderen Abhärtungstools ist es bei AppGuard weit weniger wahrscheinlich, dass die Mitarbeiter der IT/Security bei der Verwendung ihrer bevorzugten Administrationstools eingeschränkt werden. Die regelbasierte Eingrenzungs- und Isolationstechnologie benötigt nicht annähernd die gleiche Datenmenge und -genauigkeit betreffend die Hosts und ihre Anwendungen wie das HBSS. Daher kann AppGuard mit einem Bruchteil des Aufwands betrieben werden und ist für den bestehenden Serverbetrieb weit weniger störend.

Bei den meisten Sicherheitsverstößen lassen die Anwendungen Malware eindringen und/oder unterstützen das Verursachen des Schadens. Daher grenzt AppGuard Anwendungen in mehreren Ebenen ein, so dass das Betriebssystem oder andere Anwendungen nicht geschädigt werden können. Wann immer eine Anwendung eine potenziell böswillige Datei hinterlassen könnte, unterbindet AppGuard das Aktivieren und Laden von diesen Orten und leitet zu vertrauenswürdigen Quellen um. Sollte ein böswilliger Prozess es irgendwie schaffen, Zeit zum Ausführen zu gewinnen, wendet AppGuard auf die kritischsten Teile des Systems Isolationsregeln an und schützt sie vor Auswirkungen durch die böswilligen Prozesse. Dadurch ist die Malware nicht mehr in der Lage, Schaden anzurichten, obwohl sie im System Fuß fassen konnte.

Wenn Sie sich als Behörde ähnlichen Herausforderungen oder Initiativen gegenübersehen, wenden Sie sich an AppGuard, um zu erfahren, wie die patentierte Endpunkt-Absicherungstechnologie Ihr Unternehmen bei Migrationen schützen kann.

Über AppGuard

AppGuard ist ein Cybersecurity-Unternehmen, das es sich zur Aufgabe gemacht hat, einen neuen Standard zu setzen: echter Cyber-Schutz für alle.
Die patentierte Technologie von AppGuard verhindert Kompromittierungen, bevor sie geschehen, indem sie Malware-Aktivitäten daran hindert, Schaden anzurichten, ohne sie wiederkennen zu müssen.

Im Gegensatz zu erkennungsbasierten Lösungen überlistet AppGuard böswillige Akteure, damit Unternehmen ihren Aufgaben nachgehen können und die Schadsoftware nicht machen kann, was sie will.

APPGUARD
Die Malware-Defensive

www.appguard.us | software@ingrammicro.ch