KURZDARSTELLUNG: WARUM NETZWERK-SANDBOXING IM KAMPF GEGEN RANSOMWARE ENTSCHEIDEND IST

Warum Sie Sandboxing zusammen mit Signaturen und heuristischen Methoden nutzen sollten

Zusammenfassung

Next-Generation-Firewalls setzen Signaturen und heuristische Analysen mit großem Erfolg ein. Gegen die hoch entwickelten Angriffe heutiger Hacker können sie allerdings nur wenig ausrichten. Um Zero-Day-Bedrohungen und gezielte Attacken effektiv zu bekämpfen, sind Sicherheitskonzepte mit robusten Sandboxing-Funktionen wichtiger denn je.

Die wahre Herausforderung – und was Sie dagegen tun können

Das schnelle Wachstum externer Bedrohungen übertrifft heute die schlimmsten Befürchtungen. Cyberkriminelle nutzen perfide Automatisierungstechniken und versetzen sich in die Denkweise von Softwareanbietern, um ständig neue Angriffsvarianten zu kreieren – immer mit dem Ziel, einen möglichst großflächigen Schaden anzurichten, ohne dabei erkannt zu werden. Führt man sich die Folgen eines Datenlecks oder einer Ransomware-Attacke für Organisationen vor Augen, ist klar: Die Erkennung und Bekämpfung von bösartigem Code – noch bevor er das Netzwerk erreichen kann – sollte für jede IT-Abteilung zu den Top-Prioritäten gehören.

Die wahre Herausforderung ist nicht die Ransomware, die sich bereits im Internet breitgemacht hat, sondern gezielte Angriffe und Zero-Day-Bedrohungen. Bei gezielten Angriffen entwickeln Hacker für jede Organisation, die sie ins Visier nehmen, einen eigenen neuen Code. Zero-Day-Bedrohungen hingegen nutzen neu entdeckte Schwachstellen aus, für die noch keine Patches veröffentlicht wurden. Es sind vor allem diese Arten von Angriffen, um die sich Organisationen am meisten Gedanken machen müssen, da sie in der Regel – aus Sicht der Hacker – wesentlich erfolgversprechender als ältere Angriffsvarianten sind. Wie also können Sie am besten verhindern, dass eine Bedrohung sich in Ihrem Netzwerk einnistet und sich von dort ausbreitet?

Bei der Frage, wo sie bösartige Angriffe bekämpfen möchten und wie sie diese erkennen und beseitigen, stehen Ihnen ein paar Möglichkeiten offen. Ziel sollte es sein, bösartigen Code so nah wie möglich am Entstehungsort des Angriffs zu identifizieren und zu beseitigen. Wenn es darum geht, wo man einen Angriff bekämpfen sollte, kann man Organisationen grob in zwei Gruppen einteilen: Die erste setzt auf den Schutz von Endpunkten – hier gelangt der bösartige Code in ein Endgerät, wo er dann erkannt und beseitigt wird – und die zweite auf das Sandboxing – hier wird der bösartige Code identifiziert

Bösartiger Code ist heute so hoch entwickelt, dass man einen mehrschichtigen Ansatz braucht, um ihn zuverlässig zu erkennen. Allerdings haben sowohl Signaturen als auch heuristische Methoden ihre Grenzen.

und beseitigt, bevor er ins Netzwerk gelangt. Bis es eine wirklich 100-prozentige Lösung gibt, werden wahrscheinlich beide Strategien eine wichtige Rolle bei der Verteidigung spielen. Sandboxing kann – sofern richtig eingesetzt – eine präventive Wirkung haben.

So halten Sie bösartigen Code von Ihrer Organisation fern

Stellen Sie sich vor, Ihr Netzwerk wäre eine wehrhafte Burg. Die beste Stelle, um einen Angriff zu stoppen, wäre das Tor – denn hier kann man alles und jeden vor dem Einlass durchsuchen. Eine Lösung, die in der Lage ist, bösartigen Code innerhalb Ihrer Next-Generation-Firewall zu entdecken, ist vergleichbar mit einer Wache am Burgtor. Nichts kann das Tor passieren, ohne dass die Wache davon weiß. Wenn Daten Ihr Netzwerk passieren, werden sie sorgfältig durchleuchtet, um bösartigen Code aufzudecken. Dabei kommen mehrere Methoden zum Einsatz:

- Signaturen
  Der Datenverkehr wird mit einer Datenbank verglichen, die bösartige digitale Signaturen enthält. Im Falle einer Übereinstimmung wird der Code als bösartig markiert.
- Heuristische Methoden
  Im Gegensatz zum signaturbasierten Scannen, das innerhalb einer Datenbank nach Übereinstimmungen sucht, nutzt man bei heuristischen Prüfungen Regeln und Algorithmen, um potenziell bösartigen Code aufzudecken.
- Sandboxing
  Anstatt Code durchzukämmen, um bösartige Signaturen oder Aktivitäten zu identifizieren, kann man den Code in der Sandbox „detonieren“ lassen bzw. wie vom Hacker beabsichtigt ausführen. Dabei überwacht die Sandbox den Code auf bösartige Aktivitäten oder Verhaltensmuster. Dieser Prozess findet in einer speziell dafür konzipierten Umgebung – der Sandbox – statt, wo kein Schaden angerichtet werden kann.

Eine Kombination der beiden Methoden ist wesentlich effektiver, da leicht zu fassende Bedrohungen von den herkömmlichen schnelleren und weniger ressourcenintensiven Technologien identifiziert werden können. Auf diese Weise kann sich die Sandbox auf den verbleibenden Content konzentrieren, der einer strengeren Prüfung bedarf.

Signaturen und heuristische Methoden sind nicht gut genug – aber warum?

Signaturbasierte Mechanismen sind nur so gut wie die Datenbank, die sie zur Identifizierung des bösartigen Codes nutzen. Auch wenn Ihre Datenbank immer auf dem neuesten Stand ist, könnten Sie einen Angriff verpassen, weil es etwas Zeit braucht, bis Anbieter von Virenschutzlösungen Malware identifizieren, ihre Datenbank aktualisieren und Ihnen die neuen Signaturen zur Verfügung stellen. Außerdem sind Autoren von bösartigem Code mit signaturbasierten Erkennungsmethoden vertraut und nutzen daher Code, der diese umgehen kann.

Auch heuristische Methoden sind nicht immer präzise. Ein Teil des Codes könnte zum Beispiel einfach nur Datenverkehr sein, der nicht mit den erwarteten Mustern übereinstimmt. Die Folge wären Falschmeldungen. Manchmal scheint bösartiger Code zunächst nicht gefährlich zu sein, bis er im Backend wieder zusammengesetzt wird, was die Zuverlässigkeit heuristischer Methoden infrage stellt.

Nehmen wir Ransomware als Beispiel. Der zunächst heruntergeladene Code ist nicht schädlich. Gefährlich wird er erst, wenn er sich mit einem Command-and-control(C2)-Server verbindet und das Herunterladen von zusätzlichem Code veranlasst. Ein weiteres Beispiel ist ein Makro innerhalb eines Microsoft Word-Dokuments. Sofern das bösartige Makro keine verdächtige oder bekannte Angriffsmethode verwendet, lässt sich weder mit Signaturen noch mit heuristischen Methoden feststellen, ob das Makro an sich harmlos oder gefährlich ist.

Bei der passiven Prüfung des Datenverkehrs stoßen Signaturen und heuristische Methoden an ihre Grenzen. Das Scannen bietet dem Code keine Möglichkeit, aktiv zu werden. Hinzu kommt, dass Angreifer gelernt haben, schlechten Code (aus Sicht der Prüfung) innerhalb von „gutem“ Code zu verstecken. Bösartigen Code erkennt man also am besten, wenn man mit einer Version interagiert, die bereits komplett „scharf gestellt“ wurde.

Ein Spiel mit dem Feuer

Die einzige Weise, ausgeklügelten bösartigen Code zu fassen, ist ihn zur „Detonation“ zu bringen.

Dieser Prozess unterscheidet sich stark von einer einfachen Prüfung des Codes. Man könnte ihn mit der Zucht einer gefährlichen Mikrobe in einem biologischen Hochsicherheitslabor oder der Explosion einer Bombe in einem Sicherheitsraum vergleichen. Die Sandbox bietet einen sicheren Ort, an dem abgefangene Daten unter Beobachtung ausgeführt werden können. Wird verdächtiges oder bösartiges Verhalten erkannt, kann die Datei – sowie die darin enthaltene Bedrohung – eliminiert werden.

Eine Sandbox versucht, alle Dateitypen „detonieren“ zu lassen:

- Dateien mit aktiven Inhalten
  Diese Dateien enthalten ausführbare Dateien, Skripts und DLLs. Die Dateien können ausgeführt werden und mit der Sandbox normal interagieren. Auf diese Weise lassen sich bösartige Aktivitäten erkennen, wie zum Beispiel Änderungen an den OS-Firewall-Einstellungen oder die Herstellung ausgehender Verbindungen über das Internet.
- Dateien mit passiven Inhalten
  Diese Dateien enthalten beliebige Arten von Dokumenten, PDFs, komprimierte Dateien (z. B. ZIP, JZIP, RAR) und sogar Bilddateien. Sie werden mithilfe ihrer Standardanwendung analysiert, um sie auf bösartige Aktivitäten zu überprüfen. Ein Beispiel hierfür wäre ein Word-Makro, das versucht zusätzlichen Code über das Internet herunterzuladen. Ohne dass sich alle verfügbaren Softwareteile in einer Sandbox befinden, ist es unmöglich, jede passive Datei zu analysieren. Letzten Endes sollte Ihre Sandbox so konfiguriert sein, dass sie so viele Dateitypen wie möglich prüfen kann.

Malware in Bildern

Vielleicht fragen Sie sich, warum Bilddateien geprüft werden sollten, da sie zu den scheinbar unbedenklichsten Dateitypen zählen. Doch in Wirklichkeit können Bilddateien bösartige Payload-Daten enthalten. So wurde vor kurzem in Brasilien ein Angriff mithilfe eines PDF-Anhangs durchgeführt, der einen Link zu einer ZIP-Datei enthielt. Innerhalb dieser ZIP-Datei befanden sich eine ausführbare Datei und eine PNG(Portable Network Graphics)-Datei. Die PNG-Datei war klein (weniger als 64 quadratische Pixel), hatte aber eine Dateigröße von über 1 MB. Nach Prüfung der ausführbaren Datei war klar, dass der Code dazu diente, einen versteckten bösartigen Binärcode von innerhalb der PNG-Datei zu extrahieren und auszuführen.

Betrachtet man, welchen Aufwand Cyberkriminelle treiben, um ihren bösartigen Code zu verschleiern, wird die Notwendigkeit einer Sandbox und einer kontrollierten Detonation aller Dateien, die in das Netzwerk gelangen, deutlich.

Signaturen mithilfe einer Sandbox optimieren

Wie bereits erwähnt, ist ein mehrschichtiger Ansatz die beste Möglichkeit, bösartigen Code zu erkennen. Durch Verbesserung beider passiver Prüfmethoden kann der Erkennungsprozess effizienter ablaufen, da er weitaus weniger CPU-Zyklen für den Abgleich mit einer Signaturdatenbank benötigt als für die Generierung und Aufrechterhaltung einer Sandbox, die nur eine einzige Instanz bösartigen Codes „detonieren“ lassen kann.

Zusätzlich zur Detonation können mit Sandboxing Signaturen erstellt werden, wenn Code als bösartig identifiziert wird – schließlich kann die Sandbox den bösartigen Code aus unmittelbarer Nähe beobachten und prüfen. Bei Erkennung bösartigen Codes wird eine Signatur erstellt. Außerdem kann die Signaturdatenbank aktualisiert werden, was die Geschwindigkeit und Genauigkeit bei der künftigen Prüfung auf bösartigen Code verbessert.

Wenn es um die Erkennung von Bedrohungen geht, haben passive Prüftechniken dennoch ihre Schwachstellen. Die Frage, ob eine Sandbox hier effizienter arbeitet, ist also durchaus berechtigt.

Die Sandbox dient als eine Art Testumgebung, in der bösartiger Code und seine Interaktion mit dem Betriebssystem überwacht werden können. Eine Sandbox hält nach Folgendem Ausschau:

- Aufruf des Betriebssystems: z. B. Aufrufe des Überwachungssystems und API-Funktionen
- Änderungen im Dateisystem: alle Arten von Handlungen, einschließlich Erstellung, Bearbeitung, Löschung und Verschlüsselung von Dateien
- Änderungen am Netzwerk: alle Arten ausgehender Verbindungen, die nicht normal sind
- Registry-Änderungen: beliebige Änderungen, um Sicherheits- oder Netzwerkeinstellungen beizubehalten oder zu ändern
- Sonstiges: Überwachung von Anweisungen, die ein Programm zwischen Betriebssystemaufrufen ausführt, um den Kontext anderer Beobachtungen zu ergänzen

Wie effektiv sind Sandboxen?

Signaturbasierte Erkennungsmethoden eignen sich ideal, um bereits bekannten bösartigen Code aufzudecken, sind aber machtlos gegenüber Zero-Day-Angriffen oder Attacken, die einfach mutiert wurden (d. h. bestimmte Malware, die aufgrund einer Mutation mit keiner Signatur übereinstimmt). Heuristische Methoden gehen schon mal in die richtige Richtung, da sie nach unnormalen Mustern im Code Ausschau halten. Doch wie das Beispiel der Bilddatei zeigt, die zur Übertragung einer Payload genutzt wurde, lösen die Dateien im Vordergrund (z. B. ein PDF mit einem Link zu einer externen ZIP-Datei) keinen Alarm aus.

Genau dieses Problem macht die Sandbox zu so einer effektiven Erkennungsmethode. Sogar im Fall von Zero-Day-Attacken, die keine Signatur haben und nie zuvor gesehenen Code enthalten, ist Sandboxing die einzige Methode, um bösartiges Verhalten zu erkennen. Im Endeffekt führt bösartiger Code eine begrenzte Anzahl an Aktionen durch – dazu gehört die Herstellung einer externen Verbindung, das Herunterladen zusätzlicher Payloads, die Verbindung zu einem C2-Server und Änderungen am Betriebssystem. Keine dieser Aktivitäten würde man bei Dateien, die man im Büro für die Arbeit nutzt, unbedingt als normal bezeichnen.

Fazit

Es gibt verschiedene Möglichkeiten, Ihre Organisation gegen bösartigen Code zu schützen. Der Schutz von Endpunkten ist zwar wichtig. Dennoch kann sich bösartiger Code im Netzwerk einnisten und noch größere Risiken verursachen. Mit Sandboxing hingegen lassen sich Bedrohungen aufhalten, bevor sie in das Netzwerk gelangen.

Erfahren Sie mehr. Finden Sie heraus, welche Aspekte Sie bei Ihrer Sandbox-Strategie unbedingt beachten müssen. Lesen Sie unsere Lösungsübersicht „*Putting a solid sandbox strategy in place.*“ (Wie Sie eine solide Sandbox-Strategie implementieren).

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access-Security über Netzwerksicherheit bis zu E-Mail-Security: Wir haben unser Produktportfolio kontinuierlich weiterentwickelt, damit unsere Kunden Innovationen realisieren, Prozesse beschleunigen und wachsen können. Mit über einer Million Sicherheitsgeräte in nahezu 200 Ländern und Regionen weltweit bietet SonicWall seinen Kunden alles, was sie brauchen, um für die Zukunft gerüstet zu sein.

Wenden Sie sich bei Fragen zu den Nutzungsmöglichkeiten dieses Materials an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, CA 95054

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

ExecBrief-WhyNetworkingSandboxing-US-VG-24857