SONICWALL

KURZDARSTELLUNG: FÜNF BEREICHE, IN DENEN IHRE FIREWALL-SANDBOX SCHWACHSTELLEN AUFWEISEN KANN

Was Sie wissen müssen, um Advanced Persistent Threats (APTs) immer einen Schritt voraus zu sein

Unter einem Advanced Persistent Threat (APT) versteht man einen verschleierten Hackerangriff, der wiederholt durchgeführt wird und häufig auf ein bestimmtes Unternehmen abzielt. APTs enthalten in vielen Fällen unbekannte und undokumentierte Malware, einschließlich Zero-Day-Bedrohungen. Sie entwickeln sich ständig weiter, sind extrem dynamisch und kommen in vielen unterschiedlichen Formen und Varianten vor. Mithilfe solcher Angriffe können Cyberkriminelle an sensible Daten wie Identitäts-, Zugriffs- und Steuerungsinformationen gelangen und diese stehlen. Obwohl APTs nicht so häufig vorkommen wie automatisierte Angriffe oder Standardbedrohungen, die auf größere Zielgruppen abzielen, stellen sie dennoch eine ernst zu nehmende Gefahr dar.

Um APTs besser zu identifizieren, nutzen Sicherheitsexperten hoch entwickelte Technologien zur Bedrohungserkennung. Diese sind häufig mit virtuellen Sandboxen ausgestattet, die das Verhalten verdächtiger Dateien analysieren und versteckte, zuvor unbekannte Malware aufdecken. Doch Bedrohungen werden immer intelligenter und viele Anbieter können mit ihren Sandbox-Technologien einfach nicht mithalten. Diese Kurzdarstellung beschreibt fünf Bereiche, in denen veraltete Sandboxing-Technologien Schwachstellen aufweisen, und erklärt, was Ihr Unternehmen konkret braucht, um APTs immer einen Schritt voraus zu sein.

Heutige Technologien zur Erkennung raffinierter Bedrohungen melden oft nur die Präsenz und das Verhalten von Malware.

1. Malware gelangt noch vor der Analyse ins System

Manche Sandboxing-Lösungen kommen erst zu einem Analyseergebnis, nachdem eine potenziell gefährliche Datei die Netzwerkgrenzen überschritten hat. Dies erhöht die Anzahl möglicher Vektoren, die einer ausgeführten Malware-Datei zur Verfügung stehen, um Systeme innerhalb der Netzwerkgrenze zu infiltrieren.

2. Eingeschränkte Dateianalysen

Einige Gateway-Sandboxing-Lösungen können nur bestimmte Dateigrößen und -typen oder Betriebsumgebungen analysieren. Manche von ihnen sind nur für Bedrohungen ausgelegt, die auf eine einzige IT-Umgebung abzielen. Das Problem: Moderne Unternehmen verwenden mehrere Betriebssysteme wie Windows, Android und Mac OSX.

Hinzu kommt, dass die Verbreitung mobiler und vernetzter Geräte die Angriffsfläche für Hacker vervielfacht hat. 2015 beobachtete Dell SonicWALL eine große Bandbreite an neuen Angriffs- und Abwehrmechanismen, die dazu dienten, die Schlagkraft von Angriffen gegen das Android-Ökosystem – das rund 85 Prozent aller Smartphones weltweit ausmacht – zu erhöhen. Obwohl hoch entwickelt, sind heutige Technologien oft nur in der Lage, raffinierte Bedrohungen zu identifizieren und zu analysieren, die auf veraltete Office-Betriebssysteme und -Anwendungen abzielen. Somit sind Organisationen womöglich nicht vor Angriffen geschützt, die es auf moderne mobile und vernetzte Geräte abgesehen haben.

Es könnte auch sein, dass sie eine Vielzahl an Standarddateiformaten in Unternehmen gar nicht verarbeiten können, wie etwa ausführbare Programme (PE), DLL, PDFs, MS Office-Dokumente, Archive sowie JAR- und APK-Dateien. Diese Einschränkungen können dazu führen, dass unbekannte Zero-Day-Bedrohungen ohne Analyse und Identifizierung das Netzwerk passieren.

3. Isolierte Sandbox-Engines

Gegen moderne Bedrohungen sind Standalone-Sandbox-Lösungen mit einer einzigen Engine nicht mehr ausreichend.

Malware ist mittlerweile so konzipiert, dass sie die Präsenz einer virtuellen Sandbox erkennen und eine Identifizierung umgehen kann. Sandbox-Technologien der ersten Generation sind daher nur eingeschränkt effektiv. Single-Engine-Sandboxing-Lösungen lassen sich besonders leicht mit Umgehungstechniken austricksen.

Hinzu kommt, dass Single-Engine-Lösungen Lücken bei der Analyse verursachen. Zum Beispiel ist eine Analyse, bei der Aufrufe zwischen Anwendungen und Betriebssystemen geprüft werden, womöglich weniger granular als eine Analyse, bei der Aufrufe zwischen Hardware und Betriebssystemen untersucht werden, weil viele dieser Aufrufe nicht auf den Anwendungsschichten zu sehen sind.

Eine effektivere Methode besteht darin, mehrere Sandbox-Engines schichtweise zu integrieren. Trotzdem handelt es sich bei vielen Sandboxing-Lösungen heutzutage um isolierte, eigenständige Single-Engine-Appliances bzw. Cloud-Services. Die Implementierung mehrerer Sandboxing-Technologien – falls überhaupt machbar – würde die Kosten erhöhen, die Konfiguration erschweren und den Verwaltungsaufwand steigern.

4. Verschlüsselte Bedrohungen

Seit vielen Jahren setzen Finanzinstitute und andere Unternehmen, die mit sensiblen Daten arbeiten, auf das sichere HTTPS-Protokoll, das Informationen während der Übermittlung verschlüsselt. Mittlerweile verwenden noch andere Websites wie Google, Facebook und Twitter dieses Protokoll, um die wachsenden Datenschutz- und Datensicherheitsanforderungen der User zu erfüllen. Zwar bietet mehr Verschlüsselung im Internet viele Vorzüge. Der Nachteil ist aber, dass Hacker diese Verschlüsselungsmethoden ausnutzen, um Malware vor Unternehmensfirewalls zu verstecken.

Durch die Verschlüsselung mittels Secure Sockets Layer (SSL) und Transport Layer Security (TLS) bzw. HTTPS-Verkehr können findige Angreifer Command-and-Control-Kommunikationen sowie bösartigen Code präparieren, um Intrusion-Prevention-Systeme (IPS) und Anti-Malware-Systeme zu umgehen. Diese Angriffe können großen Schaden anrichten, da die meisten Unternehmen nicht über die richtige Infrastruktur verfügen, um sie aufzuspüren. Veraltete Netzwerksicherheitslösungen sind gewöhnlich nicht in der Lage, SSL-/TLS-verschlüsselten Verkehr zu prüfen, oder haben eine so schwache Performance, dass sie komplett unbrauchbar werden, sobald sie im Prüfungsmodus laufen.

5. Schwierige Problemlösung

Heutige Technologien zur Erkennung raffinierter Bedrohungen melden oft nur die Präsenz und das Verhalten von Malware. Selbst wenn die Sandbox-Lösung eine neue Bedrohung an einem bestimmten Endpunkt identifiziert, haben Organisationen in vielen Fällen keine gezielte Möglichkeit, diese Bedrohung zu beseitigen. Zudem verfügen viele Unternehmen auch über keine einfache, wirksame Methode, um Firewall-Signaturen über ein globales verteiltes Netzwerk hinweg zu aktualisieren.

Wird Malware entdeckt – was oft erst der Fall ist, nachdem das System infiziert wurde –, liegt es an der IT-Abteilung, eine Lösung zu finden. Sie muss dann die Malware nachverfolgen und beseitigen und auch etwaige Schäden an infizierten Systemen beheben. Um weitere Angriffe zu verhindern, muss die IT zudem innerhalb kurzer Zeit neue Malware-Signaturen erstellen und in der gesamten Organisation implementieren.

Welche Funktionen muss eine Sandbox bieten?

Obwohl veraltete Sandboxen Schwachstellen aufweisen, basieren sie auf einem technisch soliden Funktionsprinzip. Damit das Sandboxing effizient funktioniert, müssen diese Schwachstellen behoben werden. Ihre Sandboxing-Lösung sollte auf jeden Fall in der Lage sein:

- verdächtige Dateien einer Cloud-basierten Analyse zu unterziehen, um unbekannte Bedrohungen außerhalb des Gateways zu identifizieren und zu blockieren, bis der Sicherheitsstatus geklärt ist
- eine große Bandbreite an Dateitypen und Betriebssystemen unabhängig von Dateigröße oder Verschlüsselung zu analysieren
- Signaturen zur Problemlösung schnell und automatisch zu aktualisieren
- mehrere Sandbox-Engines zu integrieren, um nicht auf Umgehungstaktiken hereinzufallen, einen besseren Einblick in bösartige Verhaltensweisen zu gewinnen und die Bedrohungserkennung zu verbessern
- sowohl Kosten als auch die Komplexität zu verringern

Erfahren Sie mehr.

Finden Sie heraus, wie Sie durch mehrschichtiges Sandboxing mehr Zero-Day-Bedrohungen erkennen können. Sehen Sie sich diesen On-Demand-Webcast an.

> Eine effektivere Methode besteht darin, mehrere Sandbox-Engines schichtweise zu integrieren.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

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