SONICWALL™

Fünf Best Practices für einen erweiterten Schutz vor Bedrohungen

Erfahren Sie, welche Funktionen in keiner Sandbox-Umgebung fehlen dürfen.

Einleitung

Raffinierte Bedrohungen wie Zero-Day-Exploits und maßgeschneiderte Malware sind weiterhin auf dem Vormarsch. Cyberkriminelle suchen kontinuierlich nach anfälliger Software, um Schwachstellen in großen und kleinen Organisationen auszunutzen. Auf diese Weise verschaffen sie sich Zugriff auf Netzwerke, Systeme und Daten und können innerhalb weniger Minuten großen Schaden anrichten. Um diese unbekannten Bedrohungen besser zu identifizieren, nutzen Sicherheitsexperten erweiterte Technologien zur Bedrohungserkennung, wie z. B. virtuelle Sandboxen, die das Verhalten verdächtiger Dateien analysieren und versteckte Malware aufdecken.

Doch Bedrohungen werden immer intelligenter. Malware wird mittlerweile so konzipiert, dass sie virtuelle Sandboxen aufspüren und umgehen kann, was die Wirksamkeit von Technologien zur Bedrohungserkennung beeinträchtigt. Organisationen benötigen einen neuen Ansatz, um ihr Geschäft zuverlässig vor diesen raffinierten Bedrohungen zu schützen. Gefragt sind vor allem Technologien, die von bösartigem Code weder erkannt noch umgangen werden können. Um diese Anforderungen zu erfüllen, muss eine erstklassige Advanced-Threat-Protection(ATP)-Lösung folgende Funktionen bieten:

- dynamisch geschichtete Sandbox-Analysen
- Überprüfung von verschlüsseltem Datenverkehr
- Analyse sämtlicher Dateien
- Blockierung von Dateien, bis sie verifiziert werden
- schnelle Problemlösung im Falle erkannter Bedrohungen

> Moderne Sandbox-Umgebungen müssen so umfassend und dynamisch sein wie die Bedrohungen selbst, die sie verhindern sollen.

Dynamisch geschichtete Sandbox-Analysen

Multi-Engine-Sandboxen ermöglichen eine mehrschichtige Bedrohungsanalyse. Damit lassen sich Zero-Day-Bedrohungen wesentlich effektiver erkennen als mit einem Single-Engine-Ansatz. Eine Single-Engine-Sandbox kann viel leichter von der Malware entdeckt und umgangen werden. Im Idealfall umfasst eine effektive Plattform zur Bedrohungsanalyse mehrere in Schichten angeordnete Malware-Analyse-Engines. Neben virtuellen Sandbox-Umgebungen sollte diese auf jeden Fall auch Betriebssystem- und Hardwaresimulations-Sandboxing in Kombination mit einer Speicheranalyse bieten.

Eine solche Multi-Engine-Sandbox-Plattform mit virtualisiertem Sandboxing, umfassender Systemsimulation und einer Analysetechnologie auf Hypervisor-Ebene eignet sich ideal, um verdächtigen Code auszuführen. Die Plattform analysiert das Verhalten verdächtiger Dateien und macht bösartige Aktivitäten transparent, ohne sich von Umgehungstaktiken austricksen zu lassen. Außerdem sorgt sie dafür, dass Zero-Day-Bedrohungen zuverlässig erkannt werden.

Eine effiziente Lösung sollte auch das dynamische Hinzufügen zusätzlicher Schichten für die Bedrohungsanalyse ermöglichen. Da Cyberkriminelle laufend neue Wege finden, um Bedrohungen zu verschleiern, sollten Bedrohungsanalyseplattformen anpassbar sein und bei Bedarf auf neue Engines für die Bedrohungserkennung zurückgreifen können. Wie bisher werden Cyberkriminelle ihre Angriffsstrategien wohl weiterhin in atemberaubender Geschwindigkeit ändern und weiterentwickeln. Für einen umfassenden Schutz vor Zero-Day-Bedrohungen braucht man daher Lösungen, die neue Malware-Analyse-Engines dynamisch einbinden können, sobald sich die Bedrohungslandschaft ändert. Nur solche Lösungen sind effektiv genug, um die raffinierten Bedrohungen und Malware-Varianten von heute und morgen zu erkennen.

Überprüfung von verschlüsseltem Datenverkehr

Raffinierte Bedrohungen setzen heute auf komplexe und ausgeklügelte Methoden, um unerkannt zu bleiben. Sie nutzen komplett neue Konzepte oder bestehende Verteidigungsmechanismen (zum Beispiel verstecken sie sich in verschlüsseltem SSL-Verkehr). Eine Lösung zur Erkennung raffinierter Bedrohungen ist nur dann effektiv, wenn sie den gesamten Verkehr – ob verschlüsselt oder unverschlüsselt – auf verdächtige Dateien prüft. In Kombination mit einer Next-Generation-Firewall können Sandboxen SSL-Terminierungs-Technologien einsetzen, um verschlüsselte Dateien zu überprüfen. Bei Standalone-Produkten ist dieses Feature oft nicht vorhanden.

Analyse sämtlicher Dateien

Malware-Autoren verschleiern nicht nur verschlüsselten Datenverkehr – sie verstecken bösartigen Code auch in Dateien und Anwendungen. Um dagegen vorzugehen und Zero-Day-Bedrohungen zuverlässig zu erkennen, sollten Sandboxen in der Lage sein, verborgene Malware in den unterschiedlichsten Dateitypen (z. B. ausführbaren Programmen, PDFs, MS-Office-Dokumenten, Archiven, JAR- und APK-Dateien), Dateigrößen und Betriebsumgebungen (z. B. Windows, Android, Mac OS X sowie Multi-Browser-Umgebungen) zu analysieren. Für eine größtmögliche Flexibilität sollte die Lösung benutzerdefinierte Analysen nach Dateityp, Dateigröße, Absender, Empfänger und Protokoll ermöglichen und zudem eine manuelle Weiterleitung von Dateien für Analysezwecke erlauben.

Blockierung von Dateien, bis sie verifiziert werden

Zero-Day-Bedrohungen aufzuspüren ist zwar ein guter Anfang, doch damit ist es noch lange nicht getan. Eine gute Lösung sollte nicht nur den Datenverkehr auf verdächtigen Code prüfen, sondern auch die Möglichkeit bieten, diesen Code vom Netzwerk fernzuhalten, bis er analysiert wurde und der Sicherheitsstatus geklärt ist. Einige isolierte Sandboxen klären den Sicherheitsstatus erst, nachdem eine Datei in das Netzwerk gelangt ist. In diesen Fällen dienen sie eher als eine Art Alarm und nicht als vorbeugende Maßnahme.

Schnelle Problemlösung im Falle erkannter Bedrohungen

Sobald eine Bedrohung erkannt wird, kommt es auf schnelle, automatische Signaturen-Updates an. Die Wirksamkeit einer effizienten Sicherheitslösung hängt davon ab, ob sie die mühsame manuelle Pflege vereinfacht, die eine proaktive Sicherheitsstrategie erfordert. Um Folgeattacken und eine weitere Verbreitung der identifizierten Malware-Bedrohung zu vermeiden, müssen Signaturen für neu entdeckte Malware schnell generiert und automatisch über alle Netzwerksicherheitsgeräte hinweg bereitgestellt werden. Wird eine Datei in diesem Szenario als bösartig identifiziert, folgt sofort eine neue Signatur, die auf den Firewalls aufgespielt und in die Gateway-Anti-Virus- und IPS-Signaturendatenbanken sowie URL-, IP- und Domain-Reputation-Datenbanken eingepflegt wird. Ideal wäre hier ein übersichtliches Dashboard, mit dem Sie die erweiterte Bedrohungserkennung überwachen und ausführliche Analyseberichte bereitstellen können.

Fazit

Moderne Sandbox-Umgebungen müssen so umfassend und dynamisch sein wie die Bedrohungen selbst, die sie verhindern sollen. Wenn Sie von einer zuverlässigen Bedrohungserkennung, einem hocheffizienten Schutz und schnellen Reaktionszeiten profitieren wollen, sollten Sie bei der Wahl Ihrer erweiterten Sandbox-Lösung gegen Bedrohungen diese Best Practices befolgen.

Erfahren Sie, wie Sie mit SonicWall einen erweiterten Bedrohungsschutz gewährleisten können. Kontaktieren Sie uns, wenn Sie wissen möchten, wie Capture ATP Ihr Unternehmen schützen kann.

Über uns

Seit über 25 Jahren ist SonicWall als zuverlässiger Sicherheitspartner bekannt. Von Access Security über Netzwerksicherheit bis zu Email 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.
www.sonicwall.com

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

SonicWall
5455 Great America Parkway,
Santa Clara, Kalifornien (USA) 95054
www.sonicwall.com

Informationen zu regionalen und internationalen Niederlassungen finden Sie auf unserer Website.