IST IHRE ORGANISATION DER FIRST-GEN-SANDBOX ENTWACHSEN?

SANDBOXING IST EIN UNVERZICHTBARER TEIL VON ADVANCED THREAT PROTECTION

In einem kürzlich veröffentlichten Bericht wurde aufgezeigt, dass Cyber-Kriminalität die globale Wirtschaft jährlich über 450 Milliarden Dollar kostet. Weltweit wurden über zwei Milliarden persönliche Daten gestohlen – über 100 Millionen Patientendaten allein von US-Bürgern.[1] Angesichts externer Bedrohungsakteure, die für mehr als 90 % der Sicherheitsvorfälle verantwortlich sind,[2] ist es an der Zeit, darüber nachzudenken, wie eine Sandbox-Lösung im Rahmen einer umfassenderen Verteidigungsarchitektur, die für die heutigen Netzwerkumgebungen ausgelegt ist, funktionieren muss.

Es gibt heute mehr als 700 Millionen Malware-Dateien.[3] Einer der neuesten Trends ist die Einführung von Malware-as-a-Service und künstlicher Intelligenz (KI) zur Automatisierung extrem effektiver Angriffe. Dies sind einige der Hauptgründe dafür, dass die automatisierte Abwehr durch Sandboxing-Funktionen als Gegenmaßnahme Auftrieb gewinnt. Es wird erwartet, dass der weltweite Sandbox-Markt für Netzwerk-Security bis 2025 auf 40,48 Milliarden Dollar ansteigt.[4]

Netzwerke sehen sich aber nicht nur einer immer schneller wachsenden Bedrohungslandschaft gegenüber, sondern befinden sich selbst in einer Phase grundlegender digitaler Transformation. Die zunehmende Implementierung von Cloud-Technologien hat beispielsweise den Bedarf an integrierten Security-Lösungen geschaffen, die Informationen von Anfang bis Ende über verteilte Netzwerke hinweg gemeinsam nutzen. Der Übergang zur Cloud erhöht die Bandbreitenbeschränkungen am Netzwerkrand. Organisationen integrieren immer mehr Cloud-Dienste und -Umgebungen in ihre zunehmend verteilten Netzwerkinfrastrukturen und müssen daher auch die Sicherheit (z. B. Sandboxing) in diesen Umgebungen skalieren, um neu entdeckte Schwachstellen abzudecken.

Jeder dieser Faktoren, zusammen mit den sinkenden Einkaufspreisen für Sandbox-Geräte in Verbindung mit dem Anstieg von Unternehmen, die Datenpannen verhindern wollen (anstatt sie nur zu erkennen), zeigt, dass die Zeit reif ist für eine robuste Sandboxing-Renaissance.

Es gibt heute mehr als 700 Millionen Malware-Dateien.[3]

VIER ZENTRALE HERAUSFORDERUNGEN TRADITIONELLER SANDBOXING-LÖSUNGEN

Leider können nicht alle Sandboxing-Lösungen mit den heutigen Anforderungen Schritt halten – insbesondere die Sandboxen der ersten Generation oder „traditionelle" Sandboxen mit eingeschränkter Leistung und veralteten Funktionen (wie die Möglichkeit der Integration in eine breitere Security-Architektur oder erweiterte Funktionen zur Gefahrenabwehr). Die folgenden vier Hauptproblembereiche traditioneller Sandboxing-Lösungen zeigen auf, worauf bei der Implementierung einer neuen Sandbox bzw. beim Upgrade einer bestehenden Sandbox geachtet werden muss.

SICHERHEITSEFFEKTIVITÄT

Viele bekannte Sandboxing-Lösungen bieten in einer Zeit, in der es wichtiger als jemals zuvor ist, die Fenster für Erkennung und ein mögliches Eindringen zu verkleinern, nicht mehr die erforderliche Sicherheitseffektivität. Die Reaktion auf jedes Sicherheitsereignis muss sofort erfolgen, um das Risiko zu minimieren. Die Fähigkeit eines Produkts, erfolgreiche Infektionen rechtzeitig zu blockieren und zu melden, ist für die Aufrechterhaltung der Sicherheit und Funktionalität des überwachten Netzwerks entscheidend.[5]

In diesem Fall sollte die Bewertung einer Lösung nicht nur auf der effektiven Erkennungsrate für Bedrohungen basieren, sondern auch auf den Erkennungsdauer-Metriken, die sich direkt auf den ROI für Unternehmen auswirken.[6] Schnellere Erkennung von Bedrohungen und Eindämmung von Datenpannen führen zu niedrigeren Wiederherstellungskosten.

Unternehmen sind häufig gezwungen zu wählen, zwischen der Fähigkeit der Security, das Netzwerk vor allen Arten von Angriffen zu schützen, und der Fähigkeit des Netzwerks, einen hohen Durchsatz an Datenverkehr zu unterstützen. Für die sich entwickelnde Infrastruktur von heute ist jedoch ein Gleichgewicht zwischen beidem notwendig. Die Sicherheitseffektivität einer Sandbox muss im Kontext seiner Leistung beurteilt werden – und umgekehrt.[7] Organisationen müssen nach Sandboxen mit Empfehlungsbewertungen von unabhängigen Prüfunternehmen (z. B. NSS Labs) zur Sicherheitseffektivität und Erkennungsdauer suchen. Darüber hinaus ist die Effektivität einer Sandbox anhand folgender Fähigkeiten zu bewerten:

- **Integration**: Vermeiden Sie Einzelprodukte, die nicht flexibel in eine breitere Security-Architektur integriert werden können, um eine bessere Transparenz und Verwaltbarkeit zu gewährleisten. Malware ist so konzipiert, dass sie die Präsenz einer virtuellen Sandbox erkennt und eine Erkennung umgeht – wodurch die Technologien von Sandboxen der ersten Generation veraltet sind. Einige IT-Manager versuchen, dieses Problem durch die Implementierung mehrerer Sandbox-Technologien zu vermeiden, wodurch jedoch die Komplexität der Konfiguration, der Verwaltungsaufwand und die Kosten erheblich erhöht werden.[8]
- **Threat Intelligence**: Als Erweiterung der Integration benötigen Sandboxen Zugriff auf Echtzeitinformationen, die von einem erfahrenen Forscherteam (nicht nur durch Bedrohungs-Feeds von Drittanbietern) unterstützt werden, um über die neuesten Probleme weltweit informiert zu sein. Die Sandbox muss als Zero-Day-Zentrale arbeiten und die neuesten Informationen mit anderen Security-Tools und -Elementen über die gesamte Architektur hinweg teilen Nur so können koordinierte, automatisierte Reaktionen auf breite Angriffe geliefert werden. Wenn die verschiedenen Lösungen in die Security-Architektur integriert sind und Daten teilen, sind sie größer als die Summe ihrer Teile.[9]
- **Erkennen und Verhindern**: Die Erkennung eines effektiven Malware-Einbruchs muss schnell und präzise erfolgen, um Administratoren dabei zu helfen, die Infektion einzudämmen und die Auswirkungen auf das Netzwerk zu minimieren.[10] Alle Sandboxing-Lösungen enthalten irgendeine Art von Bedrohungserkennung. Sandboxen sollten jedoch auch dazu beitragen, Angriffe zu verhindern, bevor sie das Netzwerkinnere und sensible Daten erreichen. Die Abwehrfähigkeit einer Sandbox zum rechtzeitigen Blockieren und Melden potenzieller Bedrohungen ist unverzichtbar. Organisationen müssen hier nach einer Lösung suchen, die die Prävention von Sicherheitsverletzungen (auch bezeichnet als Advanced Threat Prevention [ATP] bzw. Schutz vor komplexen Bedrohungen) sowie Erkennungsfunktionen bereitstellt.
- **Selbst entwickelte Technologie.** Vermeiden Sie Sandboxen, die auf kommerziellen Technologien aufbauen, die von OEMs an viele Anbieter verkauft werden. Wenn ein Vertrag ausläuft oder ein Lizenzgeber seinen Code nicht laufend aktualisiert, kann es dazu kommen, dass Unternehmen ein unwirksames Produkt und kaum Möglichkeiten haben, das Problem zu lösen. Die effektivsten verfügbaren Sandboxing-Lösungen basieren in der Regel auf selbst entwickelten Originaltechnologien. Diese Unternehmen halten ihre Produkte gewöhnlich auf dem neuesten Stand, stellen Patches bereit und geben ihnen die neuesten und besten Funktionen die aktuelle Bedrohungslandschaft.

ADMINISTRATIONSAUFWAND

IT-Security Teams sind in der Regel mit knappen Budgets und einem weltweiten Mangel an qualifiziertem Personal konfrontiert. 45 % der Organisationen geben beispielsweise an, einen problematischen Mangel an Cyber-Sicherheitskompetenzen zu haben.[11] Security Teams sind überlastet und müssen ihre Produktivität wo immer möglich verbessern. Viele veraltete Sandboxing-Produkte erfordern manuelle Administration, wodurch die Belastung der Mitarbeiter noch erhöht wird. Bei der Wahl einer Sandbox sollten daher folgende Überlegungen berücksichtigt werden:

- **Vereinfachung des Security-Managements.** Suchen Sie nach einer Sandbox, die Zero-Day-Daten an alle internen Security Controls weitergibt, die im gesamten Netzwerk automatisch geeignete Schutzfunktionen anwenden.

Die Security Teams sind überlastet und müssen ihre Produktivität steigern.

45 % der Unternehmen geben an, einen problematischen Mangel an Cyber-Sicherheitskompetenz zu haben.[11]

Sie verbessern damit nicht nur Ihr Sicherheitsprofil, sondern eliminieren auch manuelle Vorgänge und verringern den Verwaltungsaufwand.

- **Implementierung und Formfaktoren.** Eine möglichst einfache Integration ist für US-Unternehmen bei der Kaufentscheidung für Sicherheitsprodukte die zweitwichtigste Überlegung (nach den Kosten).[12] Lösungen mit „nur vor Ort"-Formfaktoren können die Möglichkeiten einschränken, wo und wie Sandboxing eingesetzt werden kann. Lösungen, die physische Konnektoren (wie TAP-Netzwerkkomponenten) verwenden, können zudem den Zeit- und Kostenaufwand für die Implementierung von Sandboxing über eine Organisation hinweg erheblich erhöhen.

SKALIERBARKEIT

Viele traditionelle Sandboxen haben auch mit der Skalierung zu kämpfen, um den zunehmenden Datenverkehr oder infrastrukturelle Veränderungen aufgrund von Initiativen zur digitalen Transformation (z. B. Erweiterung in verschiedene Cloud-Umgebungen) zu bewältigen. Das Fehlen der neuesten technischen Möglichkeiten kann den Kauf zusätzlicher Geräte erfordern, was die Skalierung einer Sandbox-Lösung teurer und komplexer macht. Zu häufigen Skalierungsproblemen zählen auch unzureichende Leistungsfähigkeit, unerschwingliche Lizenzkosten und physische Implementierungsbeschränkungen.

- **Lizenzierung.** Zusätzlich zu den physischen Problemen veralteter Konnektoren und begrenzter Formfaktoren können übermäßig komplizierte und teure Lizenzierungsmodelle die Möglichkeit beeinträchtigen, eine Lösung wie erforderlich über eine expandierende Umgebung hinweg zu implementieren.
- **Knoten pro Cluster.** Suchen Sie nach einer Sandbox, die eine hohe Anzahl von Knoten pro Cluster unterstützt, um das Netzwerkwachstum, zunehmenden Datenverkehr und die wachsenden Sicherheitsanforderungen in der Zukunft zu antizipieren.

KOSTEN

Die Implementierung von Sandboxing kann komplex sein, wobei zahlreiche Faktoren die Gesamtkosten für Implementierung, Wartung und Instandhaltung beeinflussen.[13] Für viele Sandbox-Lösungen sind mehrere Geräte und/oder Subscriptions erforderlich, was zu hohen Gesamtbetriebskosten (TCO) führt. Die folgenden zentralen Bereiche sind zu berücksichtigen:

- **Angriffsfläche.** Ob Sie eine bestehende Lösung evaluieren, ein Upgrade durchführen oder erstmals eine Sandbox hinzufügen möchten – prüfen Sie die Vollständigkeit der Lösung und alle damit verbundenen Ausgaben. Sie sollten folgende Fragen stellen: Deckt die Sandbox die gesamte Angriffsfläche ab(Netzwerk, Endgeräte, Internet, E-Mail und Cloud) ohne zusätzliche Lizenzen und Kosten? Antizipiert sie zunehmend wichtige Funktionen wie die SSL-(Secure Sockets Layer-) und TLS-(Transport Layer Security-)Verschlüsselungsprüfung?
- **Kosten pro geschützten MBit/s.** Organisationen sollten nach Ersatz-Sandboxen suchen, die die Kosten pro geschützten MBit/s (ermittelt von unabhängigen Prüfunternehmen wie NSS Labs) reduzieren und zusätzliche Subscription-Kosten eliminieren.

JENSEITS DES TRADITIONELLEN SANDBOXING DER ERSTEN GENERATION

Sandboxen der vorherigen Generation können mit der Geschwindigkeit und Komplexität der heutigen Bedrohungslandschaft oder den durch die zunehmende Digitalisierung bedingten Veränderungen der Netzwerkinfrastrukturen nicht mithalten. Gleichzeitig bleibt Sandboxing eine dringende Notwendigkeit innerhalb einer integrierten Security-Architektur.

[1] „The Hiscox Cyber Readiness Report 2017“, Hiscox Insurance Company Inc., letzter Zugriff 21. März 2018.
[2] „2017 Verizon Data Breach Investigations Report (DBIR) from the Perspective of Exterior Security Perimeter“, Verizon, 26. Juli 2017.
[3] „Malware“, AV-TEST, 9. April 2018.
[4] „Network Security Sandbox Market Analysis By Solution, By Services (Professional Consulting, Maintenance, Subscription), By Application, By Region, And Segment Forecasts, 2014 – 2025“, Grand View Research, November 2017.
[5] „Breach Prevention Systems Test Report“, NSS Labs, 13. Dezember 2017.
[6] „NSS Labs Announces 2017 Breach Detection Systems Group Test Results“, NSS Labs, 19. Oktober 2017.
[7] „Breach Prevention Systems Report“, NSS Labs, 13. Dezember 2017.
[8] Nick Ismail, „Is your sandbox strategy keeping you safe?“, Information Age, 6. Juli 2017.
[9] Jason Pappalexis, „Breach Prevention Systems and the Importance of Interoperability“, NSS Labs, 6. Februar 2018.
[10] William Dean Freeman and Jessica Williams, „Breach Prevention Systems Test Report“, NSS Labs, 13. Dezember 2017.
[11] Jon Oltsik, „Cybersecurity skills shortage creating recruitment chaos,“, CSO, 28. November 2017.
[12] Jason Pappalexis, „Breach Prevention Systems and the Importance of Interoperability“, NSS Labs, 6. Februar 2018.
[13] „Breach Prevention Systems Test Report“, NSS Labs, 13. Dezember 2017.

HEADQUARTER
Fortinet Inc.
899 Kifer Road
Sunnyvale, CA 94086
USA
Tel.: +1 408 235 7700
www.fortinet.com/sales

VERTRIEBSBÜRO EMEA
905 rue Albert Einstein
06560 Valbonne
Frankreich
Tel.: +33 4 8987 0500

VERTRIEBSBÜRO APAC
300 Beach Road 20-01
The Concourse
Singapur 199555
Tel.: +65 6513 3730

LATEINAMERIKA ZENTRALE
Sawgrass Lakes Center
13450 W. Sunrise Blvd., Suite 430
Sunrise, FL 33323
Tel: +1 954 368 9990

Deutschland
Feldbergstraße 35
60323 Frankfurt
Deutschland
Telefon: +49 69 310 192 0

Schweiz
Riedmuehlestr. 8
CH-8305 Dietlikon/Zürich
Schweiz
Telefon: +41 44 833 68 48

Österreich
Wienerbergstrasse 11
Turm A
9.OG, 1100 Wien
Österreich
Verkaufsabteilung:
Telefon: +43 1 3760013 - 0

November 26, 2018 6:13 nachm.