SOPHOS
Security made simple.

Gezielte Angriffe effizient abwehren – mit moderner Sandbox-Technologie

Von **Anthony Merry**, Director of Product Management – Data Protection

Sowohl bei Cyberkriminellen als auch bei Unternehmen kommen immer wieder neue Tools zum Einsatz, die noch raffiniertere Angriffe bzw. noch effektiveren Schutz ermöglichen.

In letzter Zeit werden zunehmend sogenannte Advanced Persistent Threats (APTs) beobachtet. APTs wurden ursprünglich nur gegen sehr große Unternehmen eingesetzt, nehmen jetzt jedoch vermehrt auch kleine Unternehmen ins Visier. Entweder geht es darum, die kleinen Unternehmen selbst anzugreifen, oder diese werden nur als Zwischenstufe genutzt, um sich über sie Zugriff auf die Systeme und Daten größerer Unternehmen zu verschaffen.

Auch kleine und mittelständische Unternehmen geraten also zunehmend in den Fokus.

Angreifer haben kleine und mittelständische Unternehmen auf dem Radar und betrachten sie als leichte Beute, weil viele nicht die notwendigen Ressourcen und keine mehrschichtigen Abwehrmaßnahmen haben, um sich ausreichend zu schützen. 42 % aller Kleinunternehmen[2] wurden eigenen Angaben nach bereits Opfer von Cyberangriffen und die meisten betroffenen Unternehmen wurden mindestens zweimal gehackt.

Im Durchschnitt melden Kleinunternehmen den Diebstahl von etwa 30.000 € von ihren Bankkonten und die Mehrheit benötigt mindestens eine Woche, um das Problem zu beheben.

Wachsendes Bewusstsein

Positiv hervorzuheben ist allerdings, dass ein wachsendes Sicherheitsbewusstsein zu beobachten ist, da Berichte über Cyberbedrohungen immer häufiger ihren Weg in die Mainstream-Medien finden. Als Folge konnten viele Unternehmen ihren Sicherheitsstatus verbessern. Mitarbeiter erfahren aus den Medien über Cyberangriffe und entwickeln ein höheres Sicherheitsbewusstsein. Die Gefahr, dass solche Mitarbeiter sich im Internet riskant verhalten, ist demzufolge geringer. Auch die Führungsetage wird sich der drohenden Gefahr zunehmend bewusst und ist daher eher bereit, Ausgaben im Bereich IT-Sicherheit zur Verstärkung und Optimierung von Abwehrmaßnahmen zu bewilligen.

Bedarf nach umfassenden Next-Generation-Security-Lösungen

IT-Abteilungen in Unternehmen jeder Größe wissen mittlerweile, dass bei raffinierten Cyberangriffen unbekannte Malware zum Einsatz kommen kann, gegen die herkömmliche Gateway- und Endpoint-Schutzmaßnahmen machtlos sind. Um diesem Problem Herr zu werden, suchen viele Unternehmen nach neuen Lösungen. Gleichzeitig werden ergänzende Next-Generation-Sandbox-Lösungen momentan als Geheimwaffe zur Abwehr raffinierter Bedrohungen beworben.

Oftmals sind solche Lösungen jedoch zu komplex und zu teuer, sodass sie für viele Unternehmen nicht infrage kommen. Viele der komplexen Lösungen, die von größeren Unternehmen genutzt werden, können nur mit mehreren speziell für diesen Zweck vorgesehenen Geräten betrieben werden, die ressourcen- und wartungsintensiv sind. Auch arbeiten diese Lösungen oft nicht besonders genau. Daher ist ein Expertenteam erforderlich, das die Ergebnisse analysiert. Weitere Lösungen von unterschiedlichen Anbietern zu kaufen, die untereinander nicht kommunizieren, ist keine sinnvolle Strategie für eine effektiv verwaltbare Bedrohungsabwehr.

Immer mehr hochentwickelte Bedrohungen agieren im Verborgenen

74% aller Unternehmen rechnen in der nahen Zukunft mit einem APT-Angriff[3]

Advanced Persistent Threat (APT)

Ein APT ist ein Netzwerkangriff, bei dem Cyberkriminelle sich mittels individuell entwickelter, gezielter Angriffsmethoden Zugriff auf ein Netzwerk verschaffen und dort über einen langen Zeitraum hinweg unentdeckt bleiben. Während bei einfachen Angriffen der Überraschungseffekt genutzt wird (schneller Zugriff und Rückzug, um nicht erkannt zu werden), setzen APTs darauf, sich möglichst lange unentdeckt einzunisten. Hierzu nutzen sie evasive Coding-Verfahren und eine Reihe ausgeklügelter Manöver, um herkömmliche Sicherheitsbarrieren zu überwinden und sensible Daten zu stehlen.

Advanced Evasion Technique (AET)

Hierbei handelt es sich um einen Cyberangriff, bei dem unter Einsatz verschiedener bekannter Taktiken eine neue Taktik entwickelt wird, die einen von herkömmlichen Sicherheitsprodukten unentdeckten Zugriff ermöglicht. Die AET selbst richtet nicht unbedingt einen direkten Schaden an. Ihr Hauptziel ist es, dem Angreifer unbemerkt Zugriff auf ein Unternehmensnetzwerk zu verschaffen.

Neues Bedrohungszeitalter macht neue Sicherheitstechnologien wie Sandboxing erforderlich

Eine Technologie, die in der IT-Sicherheitsbranche jüngst für besonders viel Gesprächsstoff gesorgt hat, ist Sandboxing.

Sie stellen sich zum Thema Sandboxing wahrscheinlich die folgenden Fragen:

1. Was ist eine Sandbox?

2. Brauche ich wirklich eine Sandbox?

3. Warum können mich meine herkömmlichen Abwehrmaßnahmen nicht vor APTs schützen?

4. Eine solche Technologie ist doch sicher nur etwas für größere Unternehmen?

5. Noch eine Insellösung? Das klingt teuer.

6. Das klingt kompliziert. Habe ich die Ressourcen, um das Feature zu testen und bereitzustellen?

7. Wie finde ich die richtige Sandbox?

Antworten auf diese Fragen

1. Was ist eine Sandbox?

Eine Sandbox ist eine isolierte sichere Umgebung, die ein ganzes Computersystem imitiert. In der Sandbox können verdächtige Programme ausgeführt werden, um ihr Verhalten zu beobachten und ihren Bestimmungszweck nachzuvollziehen, ohne das Netzwerk eines Unternehmens zu gefährden.

2. Brauche ich wirklich eine Sandbox?

Unternehmen benötigen eine Reihe von Sicherheitstechnologien, um sich vor bekannten und unbekannten Bedrohungen zu schützen. Wahrscheinlich haben Sie bereits ein Secure Email Gateway, ein Secure Web Gateway, eine UTM oder eine Next-Generation Firewall an Ihrem Internet-Gateway bereitgestellt und auf Ihren Desktops und Servern einen Endpoint-Schutz installiert.

Selbst Anbieter, die sich auf reine Standalone-Sandbox-Technologien spezialisiert haben, würden niemals behaupten, dass ihr Produkt Advanced Persistent Threats zu 100 % erfolgreich abwehrt. Diese Anbieter geben zu, dass viele Schutzschichten erforderlich sind, um sich effektiv vor solchen Bedrohungen zu schützen.

Was Sie mit einer Sandbox erhalten, ist Ihre eigene Umgebung zur Analyse und Bekämpfung von Bedrohungen, die von den oben genannten herkömmlichen Sicherheitsverfahren unentdeckt bleiben. Raffinierte, gezielte Malware, die speziell entwickelt wurde, um nicht erkannt zu werden, wird aufgedeckt und bei ihrer sicheren Ausführung in der Sandbox blockiert.

3. Warum können mich meine herkömmlichen Abwehrmaßnahmen nicht vor APTs schützen?

Einfache signaturbasierte Virenschutzsoftware schützt Sie vor bekannter Malware. Signaturbasierter Virenschutz arbeitet jedoch ausschließlich reaktiv und kann mit modernen Angriffsszenarien immer schlechter mithalten. Deshalb ergänzen führende Anbieter ihre signaturbasierte Erkennung um eine ganze Reihe verschiedener Verfahren wie Funktionen zur Erkennung von schädlichem Datenverkehr und Emulation. Wenn Ihre Daten oder Zugangsdaten jedoch wertvoll genug für den Angreifer sind, wird dieser sich die Zeit nehmen, die Art der von Ihnen eingesetzten Sicherheitsverfahren zu ermitteln. Dann wird er seine speziell auf Sie zugeschnittene Malware testen und sicherstellen, dass diese Ihre Erkennungsmechanismen überlistet.

4. Eine solche Technologie ist doch sicher nur etwas für größere Unternehmen?

Beim Angriff auf Filialen der US-amerikanischen Supermarktkette Target wurden 40 Mio. Kreditkartennummern gestohlen. Dies erschütterte das Vertrauen in die Marke Target schwer und auf das Unternehmen kamen erhebliche Kosten zu (z. B. in Form von

Monitoring-Services zum Schutz seiner Kunden vor Betrug). Der entscheidende Punkt in diesem Beispiel ist, dass die Angreifer die Zugangsdaten von Targets Klimaanlagen-Zulieferer stahlen. Dieser kleine Zulieferer wurde als leichtes Ziel und damit als idealer Zugang zum größeren Unternehmen eingeschätzt – mit Erfolg. Daher sollten Unternehmen jeder Größe Sandbox-Technologien in Betracht ziehen; denn ein gezielter Angriff könnte sie ihre wichtigsten Kunden kosten. Laut einer aktuellen Statistik schließen 60 % aller Kleinunternehmen innerhalb von sechs Monaten nach einer Datenpanne[4].

5. Noch eine Insellösung? Das klingt teuer.

Dass eine Sandbox teuer sein kann, steht außer Frage. Aber es gibt durchaus Wege, die Kosten im Rahmen zu halten. Gartner empfiehlt in seinem Forschungsbericht zu Netzwerk-Sandboxing:

„Wenn das Budget Ihres Unternehmens begrenzt ist oder Sie nach einer schnellen Methode suchen, Sandbox-Technologie hinzuzufügen, sollten Sie zunächst Sandboxing-as-a-feature-Angebote von ihren momentanen Sicherheitsanbietern testen."

Eventuell können Sie ein Sandboxing as-a-feature-Angebot zu Ihrer UTM, Ihrer Firewall, Ihres Secure Web Gateways oder Ihres Email Gateways nutzen.

Durch die Einführung von Cloud Computing haben sich die Bereitstellungsmethoden und Preise für Rechenleistung und Speicherkapazität verändert. Unternehmen steht nun mehr Rechenleistung zu niedrigeren Preisen zur Verfügung. Dies eröffnet auf dem Gebiet der Service-Bereitstellung ganz neue Möglichkeiten, und Services wie AWS haben unser Bild von rechenintensiven Lösungen grundlegend gewandelt.

Sandboxes erweisen sich bei der Erkennung und Blockierung von APTs als äußerst wirksam, da sie eine vollständige Arbeitsumgebung für die Malware erstellen, in der diese operieren kann, ohne zu bemerken, dass sie analysiert wird. Früher mussten solche komplexen Lösungen auf einer gesonderten Hardware ausgeführt werden und erforderten die Unterstützung eines Analysten-Teams, das die Ergebnisse auswertete. Sie kamen daher nur für große Unternehmen und Malware-Analyselabore infrage.

Durch die Verlagerung in die Cloud wird Sandboxing erschwinglicher, weil Sicherheitsanbietern mehr Rechenleistung zur Verfügung steht und Ressourcen von mehreren Kunden gemeinsam genutzt werden können. Außerdem sind Unternehmen nicht mehr auf internes Fachwissen angewiesen, da ihre Anbieter oder Partner die Analysearbeit für sie an einem zentralen Ort erledigen können. Auf diese Weise werden die Kosten so weit gesenkt, dass Sandboxing-Technologie für alle Unternehmen erschwinglich wird.

6. Das klingt kompliziert. Habe ich die Ressourcen, um das Feature zu testen und bereitzustellen?

Achten Sie beim Test von Lösungen gezielt auf Produkte, die sich einfach testen und bereitstellen lassen. Cloudbasierte Lösungen können schnell installiert und sofort genutzt werden, ohne dass Hardware bereitgestellt oder Appliances upgegradet werden müssen.

7. Wie finde ich die richtige Sandbox?

Die richtige Sandbox zu finden, ist angesichts der Angebotsvielfalt alles andere als einfach. Achten Sie bei Ihrer Wahl darauf, dass die Lösung folgende Features bietet:

- **Analyse verdächtiger Objekte unterschiedlichster Art**

Entscheiden Sie sich für eine Lösung, die auch solche Bedrohungen erkennen kann, die speziell zum Umgehen von Sandboxes entwickelt wurden. Ihre Sandbox sollte in der Lage sein, verdächtige Dateien unterschiedlichster Art zu analysieren. Stellen Sie sicher, dass die Lösung Ihrer Wahl Archive, Microsoft-Office-Dokumente, PDFs und ausführbare Dateien analysieren kann.

- **Unterstützung verschiedenster Betriebssysteme und Anwendungen**

Eine breite Plattformabdeckung ist wichtig, um Malware zu erkennen, die speziell zur Ausführung in einer ganz bestimmten Umgebung entwickelt wurde.

- **Kontextinformationen über die Malware oder den gezielten Angriff**

Kontextinformationen über gezielte Angriffe sind von unternehmenskritischer Bedeutung. Sie benötigen eine Lösung, die Ihnen transparenten Schutz bietet mit detaillierten, vorfallbasierten Reports, die diesen Kontext liefern.

- **Sandbox-Analyserate**

Entscheiden Sie sich für eine Lösung, die Dateien mithilfe von Anti-Malware- und Reputationsdiensten filtert, um die Zahl fälschlich als schadhaft kategorisierter und an die Sandbox gesendeter Dateien zu reduzieren. Auf diese Weise werden die Auswirkungen auf die Performance auf ein Minimum reduziert und Ihre Benutzer nicht bei der Arbeit gestört.

- **Kollektive Sicherheitsintelligenz**

Die Lösung Ihrer Wahl sollte die kollektive Intelligenz aller Sandboxing-Ereignisse nutzen, damit Sie von Bedrohungsanalysen des gesamten Kundenstamms profitieren können. Herkömmliche Sicherheitschecks erkennen nicht alle Sicherheitsverletzungen; das Gebot der Stunde lautet deshalb, die Erkennung unbekannter Bedrohungen zuverlässiger zu gestalten. Um dies zu erreichen, muss ein kollektives IT-Sicherheitskonzept verfolgt werden, bei dem auf zentrale cloudbasierte Bedrohungsdaten („kollektive Sicherheitsintelligenz“) von einer Vielzahl von Ereignissen und Kundenimplementierungen zurückgegriffen wird.

Die neue Technologie Sophos Sandstorm

Sophos Sandstorm ist unsere Lösung zur Abwehr von Advanced Persistent Threats (APT) und Zero-Day-Malware und kann als ergänzendes Feature mit Sophos-Sicherheitsprodukten verwendet werden. Durch Einsatz leistungsstarker cloudbasierter Next-Generation-Sandbox-Technologie ermöglicht Sophos Sandstorm eine schnelle und zuverlässige Erkennung, Blockierung und Reaktion auf evasive Malware, die andere Lösungen übersehen.

Highlights:

Leistungsstarker Schutz vor gezielten Angriffen

Sophos Sandstorm bietet den leistungsstarken Schutz, den Unternehmen zur Abwehr unbekannter Bedrohungen benötigen. Dazu ist die Verwaltung einfach und der Preis erschwinglich.

Einfache Aktivierung

Sophos Sandstorm ist komplett in Ihre Sophos-Sicherheitslösung integriert. Sie müssen lediglich Ihre Subscription aktualisieren, die Sandstorm-Richtlinie anwenden und schon sind Sie vor gezielten Angriffen geschützt.

Der gesamte Vorgang dauert nur wenige Minuten.

Blockiert evasive Malware, die andere übersehen

Mit Sophos Sandstorm erkennen Sie auch unbekannte Bedrohungen, die speziell entwickelt wurden, um Sandbox-Appliances der ersten Generation zu umgehen. Mit unserem systemübergreifenden Emulationsansatz erhalten Sie einen detaillierten Einblick in das Verhalten unbekannter Malware und erkennen Malware-Angriffe, die andere einfach übersehen.

Forensik-Reports

Reagieren Sie schneller auf hochentwickelte Bedrohungen – mit einer einfachen, ereignisorientierten Analyse von Sicherheitsverletzungen. Wir liefern Ihnen nach Relevanz geordnete APT-Informationen, die auf einer Korrelation der Daten basieren. Dieser Ansatz reduziert nicht nur Störungen, sondern spart Ihnen auch Zeit.

Umfassende Analyse

Entdecken Sie potenziell schädliche Verhaltensweisen auf all Ihren Endbenutzer-Geräten und in allen kritischen Infrastrukturen. Hierzu zählen Ihre Betriebssysteme (Windows, Mac OS X und Android), physische und virtuelle Hosts, Services, Netzwerkinfrastrukturen sowie Web-, E-Mail-, Datei- und mobile Anwendungen. Bedrohungen können in der Sandstorm-Cloud sicher ausgeführt werden, sodass keine Gefahr durch Malware für Ihre Rechenzentren besteht.

Blitzschnelle Performance

Ihre Sophos-Sicherheitslösung führt eine präzise Vorfilterung Ihres Datenverkehrs durch, sodass nur verdächtige Dateien an Sandstorm gesendet werden. Auf diese Weise stellen wir sicher, dass die Latenz und Beeinträchtigung der Endbenutzer so gering wie möglich ausfällt.

Fazit

Unternehmen müssen ihre IT-Sicherheit an die immer raffinierteren und zunehmend gezielten Bedrohungen von heute anpassen. Eine Sandbox verstärkt nicht nur Ihre IT-Sicherheitsinfrastruktur, sondern bringt diese auch auf das nächste Level. Effektiv vor unbekannter evasiver Malware schützen können Sie Ihr Unternehmen nur mit einer Lösung, die sich nicht auf die Analyse von Signaturen beschränkt. Hochspezialisierte Technologien sind für viele Unternehmen allerdings zu teuer und erfordern zur Implementierung und Kontrolle besonderes Fachwissen. Sophos ändert diesen Umstand: mit einer erschwinglichen und einfach bereitzustellenden Next-Generation-Sandbox-Lösung, die für Unternehmen jeder Art geeignet ist.

Sie möchten wissen, ob Sophos Sandstorm die richtige Lösung für Ihr Unternehmen ist? Kontaktieren Sie uns – nähere Informationen finden Sie unter www.sophos.de/sandstorm.

1. Centre for Economics and Business Research (CEBR)
2. Bericht der National Small Business Association 2015
3. Ergebnisse der „Advanced Persistent Threat Awareness"-Studie der ISACA
4. Huffington Post

Jetzt kostenfrei testen

Kostenlose 30-Tage-Testversion
unter www.sophos.de/sandstorm

Sales DACH (Deutschland, Österreich, Schweiz)
Tel.: +49 611 5858 0 | +49 721 255 16 0
E-Mail: sales@sophos.de

2016-02-24 WP-DE (MP)

SOPHOS