kaspersky

Kaspersky Sandbox

Technisches Dokument

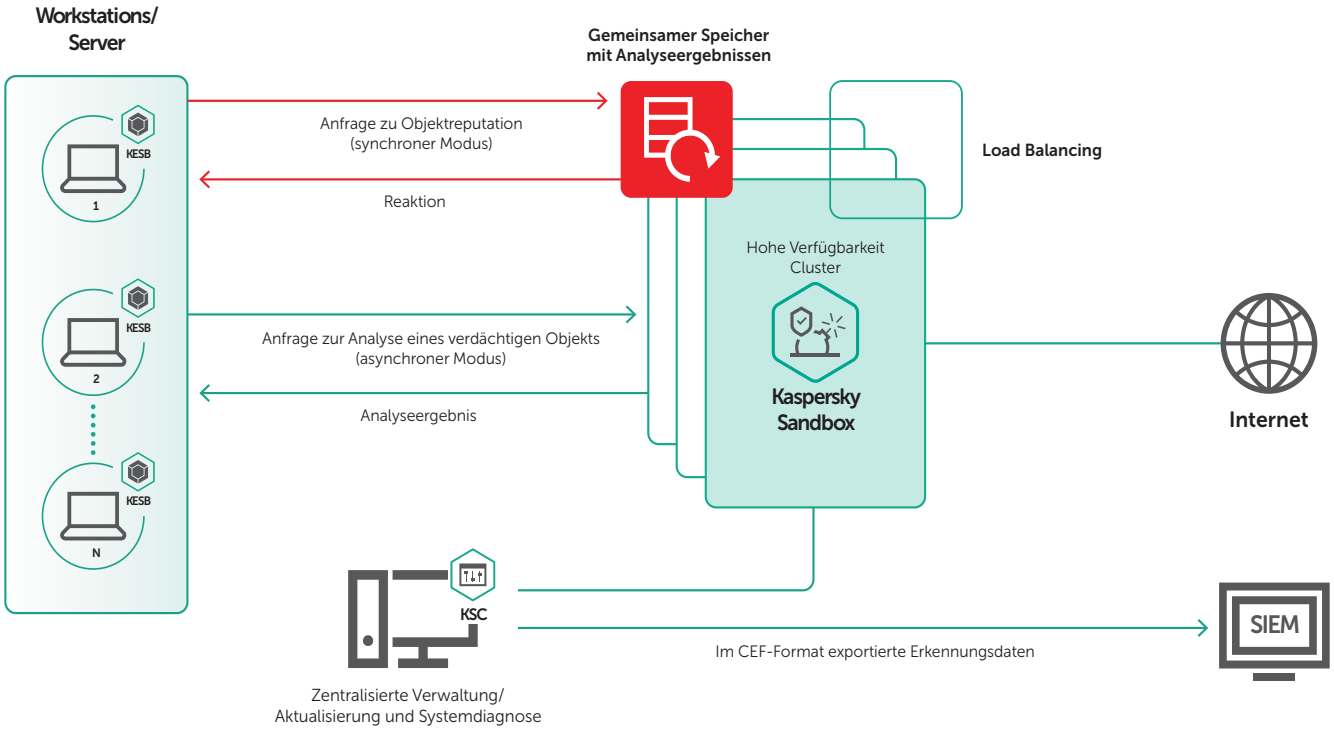
kaspersky

Einleitung

Sandbox-Technologie ist immer häufiger in Sicherheitslösungen integriert. IT-Sicherheitsexperten nutzen Sandboxes, um Verhaltensanalysen verdächtiger Objekte durchzuführen. Die Datei, z. B. ein Office-Dokument, wird auf einer virtuellen Maschine mit voll funktionsfähigem Betriebssystem und installierter Standardsoftware ausgeführt. Bei der Analyse der Objektaktionen in dieser isolierten Umgebung wird gefährliches Verhalten erkannt, daraufhin wird die Datei blockiert.

Kaspersky setzt diese Technologie bereits seit zehn Jahren als Tool zur Erkennung von Malware und zur Aktualisierung von Virendatenbanken ein. Die Sandbox-Technologie ist ein wichtiger Bestandteil der Lösungen Kaspersky Anti-Targeted Attack (KATA) und Kaspersky Threat Intelligence Portal (KTIP), der es Sicherheitsexperten ermöglicht, fortschrittliche Bedrohungen zu erkennen und schädliche Objekte zu untersuchen. Doch wie genau hilft eine Sandbox Unternehmen bei der Erkennung und Abwehr von Cyberangriffen auf ihre Workstations? In der Regel verwenden unsere Kunden Kaspersky Endpoint Security for Business (KESB), um ihre Unternehmensgeräte zu schützen. Diese Lösung kombiniert verschiedene statistische und Cloud-Analysetechnologien, um Bedrohungen zu erkennen. Mit der in KESB integrierten Sandbox erhalten unsere Kunden ein zusätzliches Modul für die dynamische Analyse des Objektverhaltens, mit dem sie fortschrittliche Angriffe automatisch erkennen und abwehren können.

Die Architektur der Lösung



kaspersky

Beschreibung

Die Lösung umfasst drei Komponenten:

1. Kaspersky Sandbox-Servercluster
2. Kaspersky Endpoint Security for Business (KESB)
3. Kaspersky Security Center (KSC)

Die gescannten Objekte werden vom Sandbox-Servercluster auf einer isolierten virtuellen Maschine ausgeführt, die eine Workstation simuliert. Die Komponente erhält eine Anfrage zur Dateianalyse von einem KESB Agent, der auf dem Gerät des Endbenutzers installiert ist. Daraufhin wird das Objekt in die Warteschlange eines der Server im Cluster verschoben. Wenn eine Datei zur Verarbeitung gesendet wird, führt Kaspersky Sandbox sie aus und protokolliert alle Aktionen der Datei. Die Komponente analysiert die gewonnenen Daten auf verdächtige oder schädliche Aktivität und gibt das Ergebnis an den KESB Agent zurück, der den Scan angefordert hat.

Darüber hinaus wird das Ergebnis der Dateiprüfung an einen gemeinsamen Speicher gesendet, über den auch andere Hosts schnell Informationen zum gescannten Objekt abrufen können, ohne es erneut analysieren zu müssen. Diese Vorgehensweise reduziert die Auslastung der Sandbox-Server und verbessert die Reaktionszeit bei neuen Bedrohungen.

Kaspersky Endpoint Security for Business erkennt verdächtige Dateien im On-Access-Modus (aktualisierbare Logik; wird gemeinsam mit Datenbanken und anderen Systemkomponenten aktualisiert) und kann daraufhin über zwei verschiedene Modi einen Objektscan anfordern: synchron oder asynchron.

Im synchronen Modus fordert der KESB Agent Daten zu einer Datei vom gemeinsamen Speicher mit Analyseergebnissen ab. Wenn das Objekt bereits gescannt wurde, erhält KESB das Ergebnis dieses Scans und kann die Datei daraufhin blockieren oder sie als sicher markieren.

Wenn kein Ergebnis abgerufen werden kann, startet der KESB Agent den nächsten Scanmodus, sendet die verdächtige Datei an Kaspersky Sandbox und wartet daraufhin im asynchronen Modus eine Antwort ab. Während der Sandbox-Analyse wird dem Objekt das Ergebnis seiner Überprüfung angehängt. Basierend auf diesem Ergebnis blockiert der KESB Agent die Datei oder markiert sie als sicher – ganz wie im synchronen Modus.

Das Kaspersky Security Center (KSC) erfüllt verschiedene Funktionen:

1. Verwaltet KES-Richtlinien, die in diesem Fall die Verbindungseinstellungen des Kaspersky Sandbox-Clusters enthalten.
2. Erfasst Statistiken zu den Ergebnissen der Sandbox-Scans und leitet diese Ergebnisse in Form von Berichten an den Systembetreiber weiter.
3. Verwaltet die Komponenteneinstellungen und Lizenzen von Kaspersky Sandbox.
4. Ruft Statistiken zum Betrieb der Sandbox-Server ab und leitet diese Daten in Form von Berichten an den Systembetreiber weiter.
5. Überträgt Informationen zu Kaspersky Sandbox-Erkennungen an SIEM-Systeme (im CEF-Format).

Bereitstellungsformat der Lösung

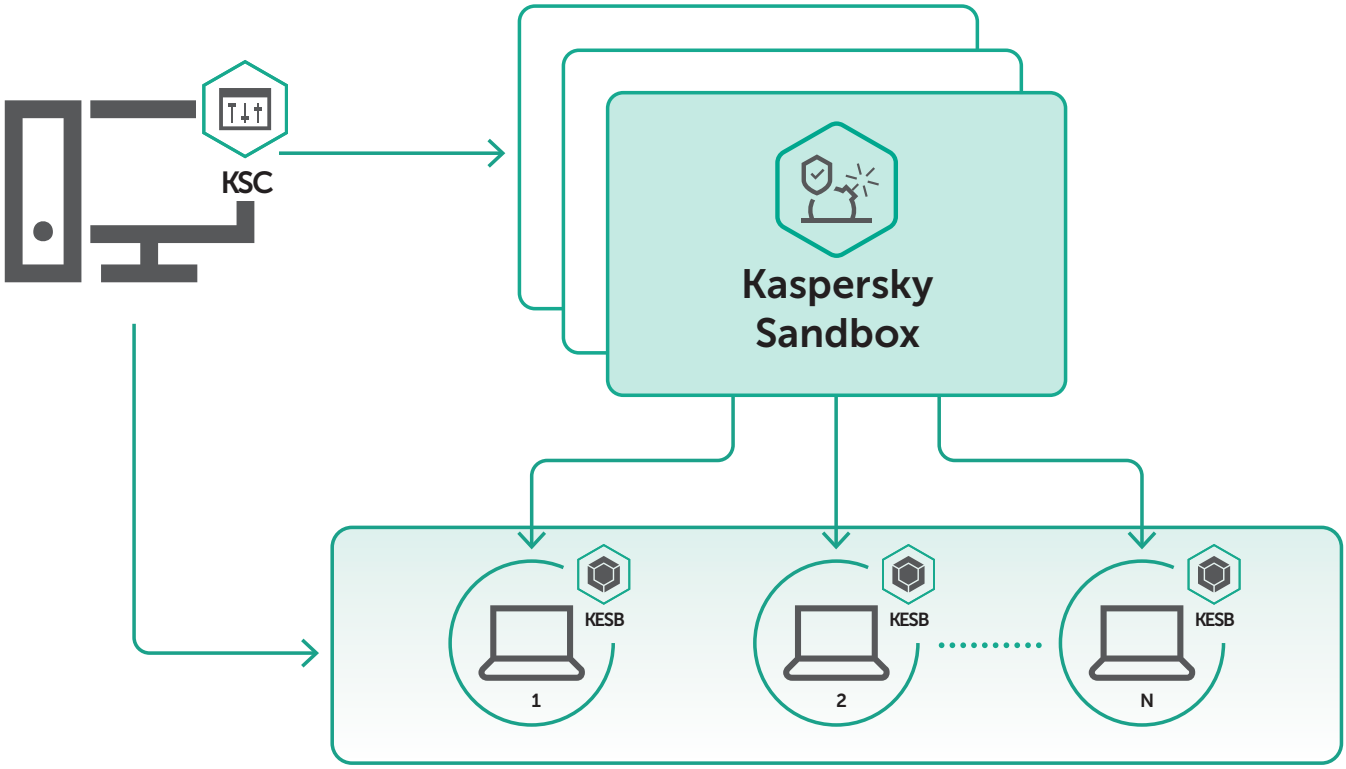
Kaspersky Sandbox wird als ISO-Image bereitgestellt, das Folgendes beinhaltet:

- Vorkonfiguriertes Betriebssystem CentOS 7 (oder höher)
- Lösungskomponenten
  - Kaspersky Network Agent KSC 11
  - Image der virtuellen Windows-Maschine mit aktiviertem Windows 7 (64 Bit)
  - Im Windows-Image enthaltene Programme: Adobe Reader, Adobe Flash Player, Microsoft Office, Internetbrowser, Java, Microsoft .NET usw.

kaspersky

Standardkonfigurationen

1. Unternehmen ohne Zweigstellen



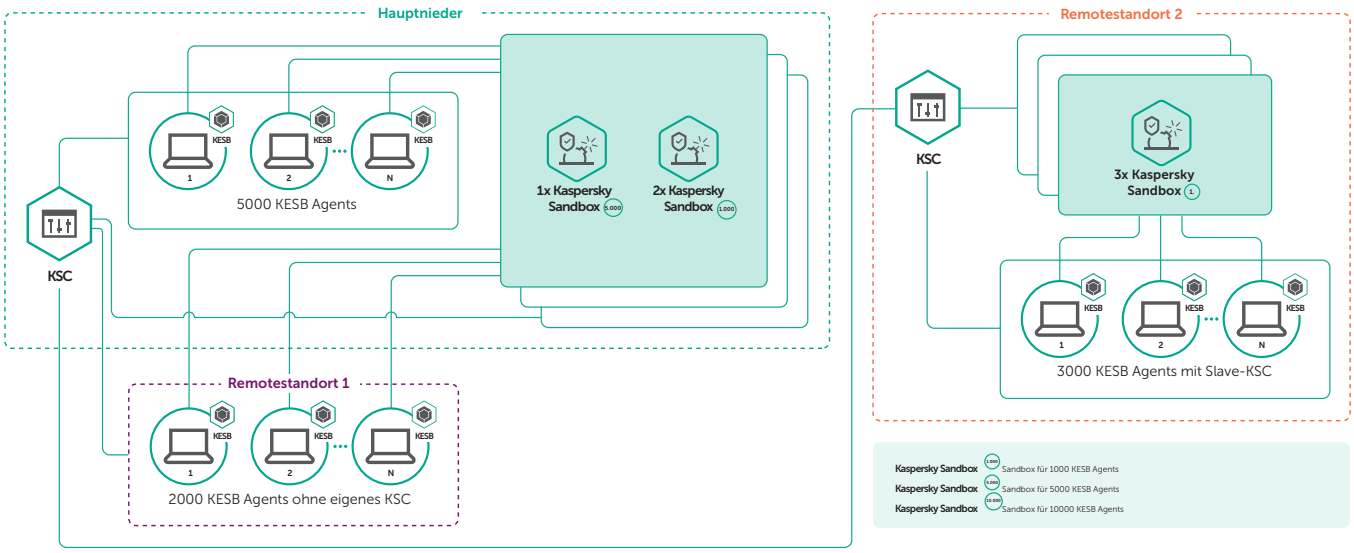
Unternehmen ohne Zweigstellen und mit 3000 KESB-geschützten Endpoints

Dank der Kommunikationskanäle kann der zentralisierte Kaspersky Sandbox-Cluster als zentraler Softwareservice eingesetzt werden, der auch Remotestandorte Ihres Unternehmens unterstützt.

Die erforderliche Anzahl an Kaspersky Sandbox-Servern wird anhand der Anzahl verbundener KESB Agents bestimmt. Diese Server werden daraufhin in einem Cluster mit einem gemeinsamen Speicher vereint.

kaspersky

2. Unternehmen mit Hauptsitz und mehreren Niederlassungen



Große Unternehmen mit 10 000 KESB-geschützten Hosts

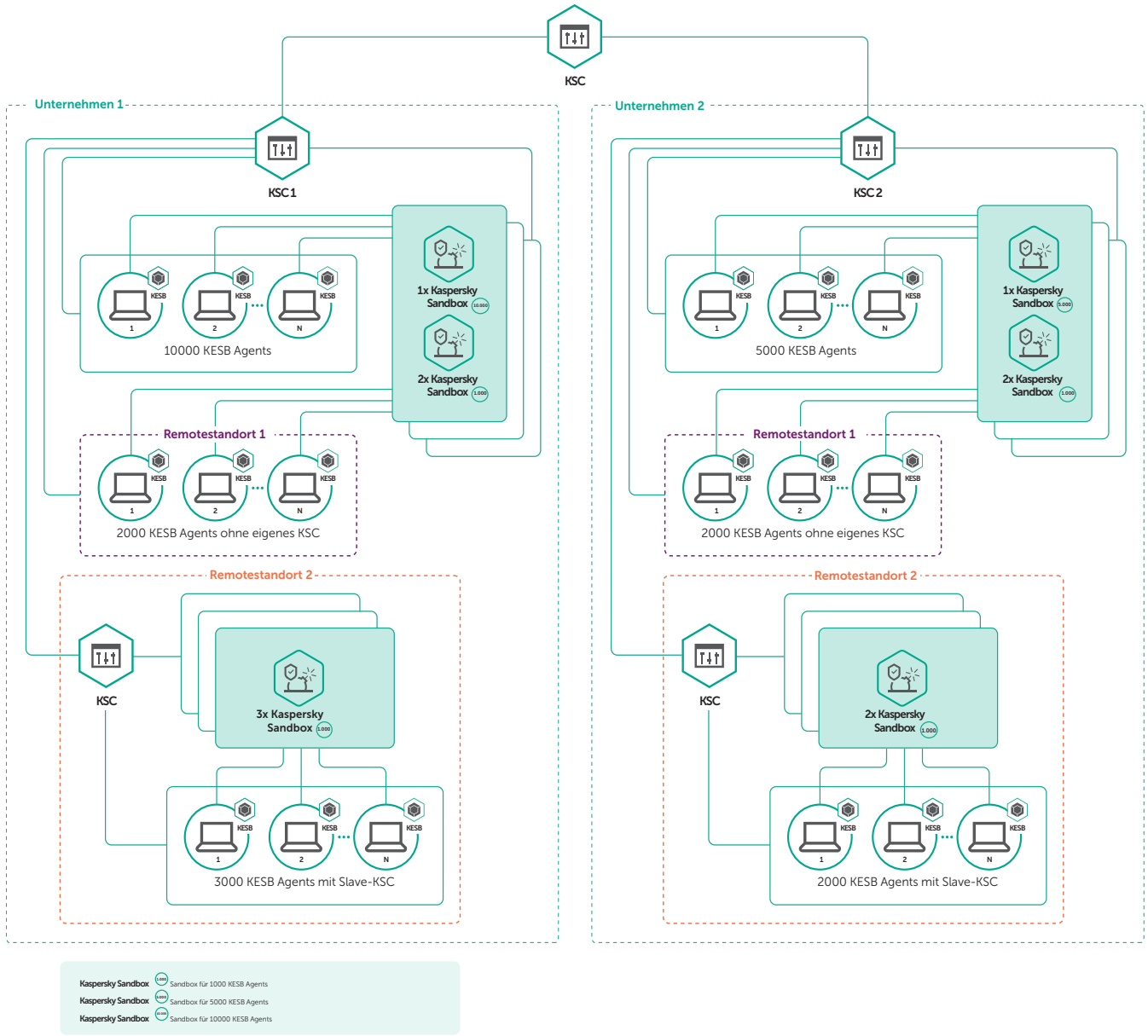
Das Unternehmen betreibt einen Hauptsitz mit 5000 Hosts, eine regionale Zweigstelle mit 2000 Hosts und guter Verbindung zum Hauptsitz sowie eine große Niederlassung mit 3000 Hosts, aber schlechter Verbindung zum Hauptsitz.

In dieser Art von Unternehmen kann ein Kaspersky Sandbox-Cluster (z. B. mit 5000 Hosts und zwei Servern für 1000 Hosts) verwendet werden, um Hauptsitz und regionale Zweigstelle zu schützen, während ein separater Cluster aus drei Kaspersky Sandbox-Servern für 1000 Hosts die Niederlassung mit der schlechten Verbindung zum Hauptsitz schützt.

In diesem Fall wird der Cluster, der die Kaspersky Sandbox-Server für Hauptsitz und regionale Zweigstelle enthält, von einem KSC-Server verwaltet, der im Hauptsitz installiert ist. Die Sandbox-Server der großen Niederlassung werden hingegen von einem separaten KSC-Server gesteuert, der in der lokalen Infrastruktur installiert wird

Wenn es die Qualität der Verbindung zulässt, können die KSC-Server in einer Hierarchie mit beiden Kaspersky Sandbox-Clustern zusammengeführt werden, die zentral vom Hauptsitz aus verwaltet wird.

3. Unternehmen mit vielen Zweigstellen und Niederlassungen



Dieses Unternehmen betreibt viele Zweigstellen und Niederlassungen verschiedener Größe oder ist MSP-Anbieter, der viele Kundenunternehmen schützt.

In diesem Fall wird eine komplexe Hierarchie von KSC-Servern verwendet, um die KESB Agents zu verwalten. Basierend auf der Anzahl geschützter Hosts wird ein separater Kaspersky Sandbox-Cluster in den einzelnen Niederlassungen des Unternehmens installiert.

Darüber hinaus können mehrere Unternehmen mit einem Cluster verbunden werden, wenn sie über einen einzelnen KSC-Server verwaltet werden.

kaspersky

4. Installation auf einem virtuellen Server

Kaspersky Sandbox kann auf virtuellen Servern installiert werden, die auf VMware ESXi. Diese Installation nutzt einen Hardwareprozessor-Passthrough und reduziert so die Anzahl der Prozessoren in der virtuellen Maschine auf die Anzahl der Threads auf dem ESXi-Server. In dieser Installation steigen die Anforderungen hinsichtlich der Serverressourcen von Kaspersky Sandbox um ca. 50 Prozent. Mit dieser Konfiguration kann Kaspersky Sandbox in Unternehmen implementiert werden, die eine virtuelle Infrastruktur bevorzugen.

5. Failover

Für jedes Bereitstellungsschema kann eine Failover-Konfiguration erstellt werden. Basierend auf der Anzahl verbundener KESB Agents kann der Kaspersky Sandbox-Cluster zwischen einem und drei zusätzlichen Servern enthalten. Unterstützende Server übernehmen die Dateiverarbeitung, wenn Kaspersky Sandbox-Nodes ausfallen.

Typische Anwendungsfälle

Szenario 1

Ein Benutzer, bei dem KESB installiert ist, erhält eine E-Mail mit einem angehängten Dokument, das einen Zero-Day-Exploit enthält. Das Dokument wird an Kaspersky Sandbox gesendet, wo es in einer isolierten Umgebung geöffnet wird, die eine reale Workstation simuliert. Die schädliche Payload wird protokolliert, während sie vom Malware-Server heruntergeladen wird. Bei der Sandbox-Analyse des Dokumentverhaltens wird das Objekt als schädlich erkannt. Im Vergleich zur Standardversion von KESB protokolliert Kaspersky Sandbox die Aktivität von Bürosoftware ausführlicher und erkennt Exploits deutlich effizienter.

Szenario 2

Cyberkriminelle verschaffen sich Fernzugriff auf die Infrastruktur des Unternehmens und installieren über legitime Tools Malware auf Netzwerkgeräten. Der KESB Agent erkennt die Bedrohung und sendet die installierbare Datei zum Scan an Kaspersky Sandbox. Nachdem dem Objekt das Ergebnis seiner Überprüfung angehängt wurde, blockiert KESB die Datei auf allen Geräten, auf denen eine Installation versucht wird.

Szenario 3

Ein Unternehmen wird Opfer eines Massen-Spam-Angriffs, dessen Nachrichten schädliche Anhänge enthalten. Die Workstations des Unternehmens sind nicht mit dem Kaspersky Security Network, unserer globalen Cloud-Reputationsdatenbank, oder dem Kaspersky Private Security Network, der privaten Version des Kaspersky Security Network, verbunden und daher nicht geschützt. Dank der automatischen Objektverarbeitung reduziert Kaspersky Sandbox deutlich das Risiko, dass gefährliche Anhänge auf Unternehmensgeräten geöffnet werden. Die Dateianhänge der Nachrichten werden an die Sandbox gesendet und dort als schädlich eingestuft. Daraufhin erhalten alle KESB Agents auf den Endgeräten das Ergebnis dieser Einstufung über den gemeinsamen Speicher und blockieren die entsprechende Datei.

Szenario 4

In manchen Fällen werden die KESB-Technologien zur Verhaltensanalyse auf Clients deaktiviert (dies wird nicht empfohlen). Hier kann Kaspersky Sandbox durch die dynamische Analyse des Objektverhaltens das Risiko reduzieren, dass Malware in Unternehmensgeräte eindringt.

Szenario 5

Im Gegensatz zu KESB analysiert die in Kaspersky Sandbox integrierte Intrusion-Detection-Komponente nicht nur eingehenden, sondern auch ausgehenden Datenverkehr der untersuchten Datei. Diese Technologie eignet sich optimal dazu, Bots zu erkennen, da sie die Kommunikation zwischen Malware und C&C-Server überwacht.

Szenario 6

Kaspersky Sandbox bietet eine API als Schnittstelle zu Drittanbieterprogrammen. Diese API ist nützlich, wenn das Unternehmen eine eigene Abteilung für Informationssicherheit sowie ein eigenes SOC betreibt.

kaspersky

Integrationsfunktionen

SIEM-Systeme können Informationen zu KESB-Erkennungen aus Kaspersky Sandbox abrufen. Diese Informationen werden im Rahmen der allgemeinen KESB-Ereignisübertragung über das KSC gesendet. Kaspersky Sandbox enthält eine API für die Integration in andere Lösungen, die folgende Möglichkeiten bietet:

- Dateien zum Scannen an Kaspersky Sandbox senden
- Informationen zur Dateireputation von Kaspersky Sandbox abrufen

Entwicklungspläne

Der wichtigste Vorteil von Kaspersky Sandbox liegt darin, dass die Lösung die Zahl der Erkennungsszenarien steigert, wenn sie in andere Sicherheitslösungen implementiert wird. Deshalb ist die weitere Entwicklung von Kaspersky Sandbox stark auf die Unterstützung von Integrationsszenarien mit bestehenden und geplanten Kaspersky-Produkten ausgelegt.

Hier die wichtigsten Integrationspläne für 2020:

- Automatische Generierung von Gefährdungsindikatoren, oder IoCs (Indicators of Compromise), basierend auf den Ergebnissen der Objektscans in Kaspersky Sandbox sowie auf Scans aller Hosts im System mithilfe von EDR-Tools
- Integration in Kaspersky Hybrid Cloud Security (KHCS)
- Integration in Kaspersky Security for Windows Server (KSWS)

Auch geplant:

- Integration in Kaspersky Security for Mail Gateway (KSMG) und Kaspersky Web Traffic Security (KWTS)
- Unterstützung für OEM-Bereitstellung

kaspersky

www.kaspersky.de
de.securelist.com