KASPERSKY PRIVATE SECURITY NETWORK

Cloud-basierte Cybersicherheit in Echtzeit für Netzwerke, deren Nutzung durch Datenschutz- oder Compliance-Bestimmungen eingeschränkt ist

Standardsicherheitslösungen benötigen bis zu vier Stunden, um die von Kaspersky-Analysten täglich entdeckten, über 325.000 neuen Schadprogramme zu erkennen, zu erfassen und abzuwehren. Das Kaspersky Private Security Network benötigt hierfür ca. 40 Sekunden – ohne dass dabei ein einziger Datensatz Ihr Netzwerk verlässt.

Das Kaspersky Private Security Network kann im eigenen Rechenzentrum eines Unternehmens installiert werden; Ihre internen IT-Spezialisten behalten die vollständige Kontrolle. Sie profitieren von den Vorteilen der cloudgestützten Sicherheit, ohne die Einhaltung Ihrer Datenschutzrichtlinien zu gefährden.

GEEIGNET FÜR:

- Unternehmenskunden mit strengen Datenkontrollvorschriften
- Staatliche Stellen und Organisationen
- Telekommunikationsunternehmen
- Service Provider

HAUPTVORTEILE

- Den Ursprung von Malware identifizieren und die Ausbreitung verhindern
- Den durch Cybersicherheitsvorfälle hervorgerufenen Schaden minimieren
- Die Anzahl von Fehlalarmen verringern
- Zwischen gezielten Angriffen und allgemeinen Bedrohungen unterscheiden
- Anforderungen an Vorfallsuntersuchung und Korrekturmaßnahmen überprüfen

Wichtigste Vorteile

ALLE VORTEILE DER CLOUD-BASIERTEN SICHERHEIT, OHNE DASS VERTRAULICHE INFORMATIONEN IHR LOKALES NETZWERK VERLASSEN:

- Einzigartige Einblicke in die neusten und raffiniertesten Cyberbedrohungen, bereitgestellt über die kontrollierte Umgebung Ihres lokalen Netzwerks
- Behördliche Auflagen, Sicherheits- und Datenschutznormen einhalten
- Isolierung kritischer Netzwerke, einschließlich Anforderungen an „Luftschleusen"
- Echtzeitschutz vor hoch entwickelten Bedrohungen, ohne dass Daten dabei das Unternehmen verlassen
- Flexible Optionen für Deployment und Pilotprojekte
- Auf MSSP/ISP-Installation vorbereitet

Das Kaspersky Private Security Network kann einfach getestet und bereitgestellt werden: Sie benötigen lediglich 1 bis 2 Standardserver, um von Bedrohungsinformationen in Echtzeit profitieren zu können.

Funktionen

GLOBALE BEDROHUNGSINFORMATIONEN FÜR PRIVATE NETZWERKE

Aktuelle Bedrohungsinformationen in Echtzeit. Verbesserung von Schutz, Erkennung und Reaktionszeiten und weniger Fehlalarme dank optimaler Reputationsanalyse. Datei-Hashes, reguläre Ausdrücke für Verhaltensmuster von URLs und Malware werden zentral gespeichert und kategorisiert, um schnell verfügbar zu sein.

DATEIREPUTATIONSDIENST

Der Kaspersky Private Security Network-Dienst liefert anhand des Hashwerts Informationen über Dateien. Sie erhalten u. a. folgende Angaben:

- Dateieinschätzung: Einwandfrei/Schädlich/Unbekannt
- Dateikategorie: Browser/Entwickler-Tools/Unterhaltung/Internet/Multimedia/Netzwerk/BS & Dienstprogramme usw.
- Digitale Dateisignatur
- Popularität der Datei

Die Einschätzungen und Kategorien werden mit der laufend aktualisierten dynamischen Whitelist von Kaspersky Lab abgeglichen, die über eine Milliarde Dateien enthält. So wird eine präzise Blockierung von schädlichen oder unerwünschten Dateien mit wenigen Fehlalarmen möglich.

URL-REPUTATIONSDIENST

Der URL-Reputationsdienst des Kaspersky Private Security Network liefert Informationen über sichere und schädliche Online-Ressourcen (z. B. Webseiten mit schädlichen Links, Malware oder Phishing):

- Einschätzung: Einwandfrei/Schädlich/Unbekannt
- Kategorie: Phishing/Malware/Web-Mail/Online-Shopping/Soziale Netzwerke/Webseiten mit Stellenangeboten/Nicht-jugendfreie Inhalte/Spiele/Glücksspiele usw.

MUSTERBASIERTE ÄHNLICHKEIT

Erkennt das Verhalten von Programmen mithilfe von Kaspersky-Produkten, erstellt ein heuristisches Muster zu dessen Identifizierung bzw. etwaiger Manipulationen daran.

EINHALTUNG VON SICHERHEITSSTANDARDS FÜR DIE NETZWERKISOLIERUNG

Das Kaspersky Private Security Network wird vollständig innerhalb des Sicherheitsperimeters eines Unternehmens installiert und bleibt auf diese Grenzen beschränkt. Auf diese Weise können auch Unternehmen mit strikten Datenschutzauflagen – z. B. Finanzdienstleister oder Behörden – von cloud-basierter Sicherheit profitieren, ohne Kompromisse beim Datenschutz einzugehen.

MSA ENTERPRISE INBEGRIFFEN

Jede Installation beinhaltet ein Maintenance- und Support-Agreement (MSA) einschließlich 24x7x365-Services mit höchster Priorität, 30 Minuten Reaktionszeit[1] und eigenem Kaspersky Technical Account Manager.

SYSTEMANFORDERUNGEN

Das Kaspersky Private Security Network ist eine software-basierte Lösung zur Installation auf physischen oder virtualisierten Servern.

Serverkonfiguration:
2 Einheiten (4 bei Hochverfügbarkeitskonfiguration):

- Datei + URL-Reputation: 1 Einheit
- Server für andere KPSN-Dienste: 1 Einheit

Konfiguration der Servereinheit:

- 2 CPUs – 3,3 GHz, 4 Kerne
- 256 GB RAM
- 300 GB Festplattenspeicher

Netzwerkanforderungen:
Zwei Netzwerkschnittstellen mit jeweils 1 Gbit/s.

Software-Anforderungen:

- Debian OS v8.2
- Google Chrome™, Mozilla™ Firefox™ oder Opera als Browser
- Java-Plug-in, Version 7 oder höher.

[1] Zeitraum zwischen Vorfallsprotokollierung und Bereitstellung einer qualifizierten Reaktion bei Vorfällen vom „Schweregrad 1"

Kaspersky Private Security Network/Version 1.0/Oktober 2015/Global