KASPERSKY lab

Kaspersky Security Network

Das Kaspersky Security Network (KSN) ist eine komplexe verteilte Infrastruktur für die intelligente Verarbeitung sicherheitsrelevanter Datenströme von Millionen freiwilliger Teilnehmer weltweit. Durch die automatische Analyse dieser Datenströme in der Cloud garantiert das System schnelle Reaktionszeiten auf neue und noch unbekannte Cyberbedrohungen und gewährleistet den bestmöglichen Schutz für jeden Partner oder Kunden.

Das KSN verfolgt das HuMachine-Prinzip von Kaspersky Lab: Eine Kombination unseres Expertenwissens und unserer lernfähigen Systeme der nächsten Generation ermöglicht es uns, Muster, Veränderungen und neue Bedrohungen in der Cyberlandschaft präzise und sorgfältig zu erkennen.

Schutz vor unbekannten und hoch entwickelten Cyberbedrohungen

Das Internet ist aus unserem Leben nicht mehr wegzudenken, es ist jedoch auch eine Quelle wachsender Risiken. Allein im ersten Quartal 2017 entdeckten Sicherheitslösungen von Kaspersky Lab 479 Millionen böswillige Angreifer und 51 Millionen Phishing-Versuche auf Nutzergeräten – beinahe doppelt so viel wie im ersten Quartal 2016. Die Cyberkriminalität nimmt nicht nur stetig zu, sie wird auch immer raffinierter. Statistiken von Kaspersky Lab zeigen, dass es sich bei 70 % der Bedrohungen, denen Nutzer jeden Tag ausgesetzt sind, um bekannte Malware handelt, während 30 % unbekannte, hoch entwickelte Bedrohungen sind, gegen die ein zusätzlicher Schutz notwendig ist. Die zunehmende Zahl und Komplexität der Bedrohungen erfordern eine spezielle Herangehendweise an die Cybersicherheit. Ein konventioneller On-Premise-Schutz reicht nicht länger aus, daher kommt heute bei allen führenden Sicherheitsanbietern ein Hybridschutz zum Einsatz. Dabei handelt es sich um eine Kombination aus Geräte- und Cloud-basierten Technologien.

Diese Herangehensweise vereint die Vorteile konventioneller Schutzmethoden, wobei deren Defizite auf ein Mindestmaß reduziert werden, mit dem Potenzial globaler Überwachung sowie kontinuierlich aktualisierten Informationen über neue Bedrohungen. Der Cloud-Schutz bietet vier Hauptvorteile:

- Bessere Erkennungsrate
- Schnelle Reaktionszeit auf neue Bedrohungen
- Minimierung von Fehlalarmen
- Ein benutzerfreundliches Produkt

Grundlegende Prinzipien des Kaspersky Security Network

- Die verarbeiteten Informationen beschränken sich auf das, was zur Verbesserung des Erkennungsalgorithmus, Optimierung des Produktbetriebs und Bereitstellung der besten Lösung für unsere Kunden erforderlich ist;
- Wir erhalten die verarbeiteten Informationen von Kunden, die einer Endbenutzer-Lizenzvereinbarung und einer KSN-Vereinbarung zugestimmt haben. Im Rahmen dieser Dokumente werden die erfassten Informationen ausführlich beschrieben[1];
- Die Zustimmung zur KSN-Vereinbarung kann jederzeit in den Einstellungen erteilt oder widerrufen werden;
- Die durch das KSN erfassten Daten können keiner Einzelperson zugeordnet werden. Die Informationen werden in Form von aggregierten Statistiken auf separaten Servern mit strengen Richtlinien bezüglich der Zugriffsrechte verwendet;
- Die geteilten Informationen werden auch bei der Übertragung gemäß gesetzlichen Anforderungen und strikten Branchenstandards wie Verschlüsselung, digitale Zertifikate, Firewalls etc. geschützt.

Kaspersky Security Network-Workflow

Die Funktionsweise des Kaspersky Security Network umfasst verschiedene Hauptprozesse, darunter die unterbrechungsfreie weltweite Überwachung realer Bedrohungen auf Nutzergeräten, die Analyse erfasster Daten zur Erkennung neuer Bedrohungen sowie die Bereitstellung relevanter Lösungen und Gegenmaßnahmen an geschützte Kunden. Die Informationen über Infektionsversuche werden mithilfe der umfangreichen internen Sachkenntnis des Unternehmens und technischer Ressourcen analysiert – sowohl durch Mitarbeiter als auch durch automatisierte Vorgänge.

Die Sicherheit eines Programms wird mit vielschichtigen Tests unter Einsatz von lernfähigen Systemen bestimmt. Diese beinhalten die Prüfung der Reputation des Verhaltens in der Cloud – dabei werden die potentielle Gefährlichkeit, die Quelle und die Integrität des Programms sowie viele weitere Faktoren unter die Lupe genommen.

Zur Bestimmung der Sicherheit einer Webseite wird das digitale Zertifikat des Unternehmens geprüft und dessen Legitimität bestätigt, der Inhalt der Webseite auf potentielle Gefahren und Fallen untersucht, die Reputation der URL in der Cloud geprüft sowie viele weitere Faktoren durchleuchtet.

Sobald die Legitimität eines Programms oder eine Webseite bestätigt wurden, erfolgt ein Eintrag in die Liste vertrauenswürdiger Anwendungen oder Webseiten (der Whitelisting-Datenbank). Gilt ein Programm oder eine Webseite als schädlich, erfolgt eine Meldung an das „Urgent Detection System“ von Kaspersky Lab, und die Informationen werden allen Nutzern über das Kaspersky Security Network zur Verfügung gestellt.

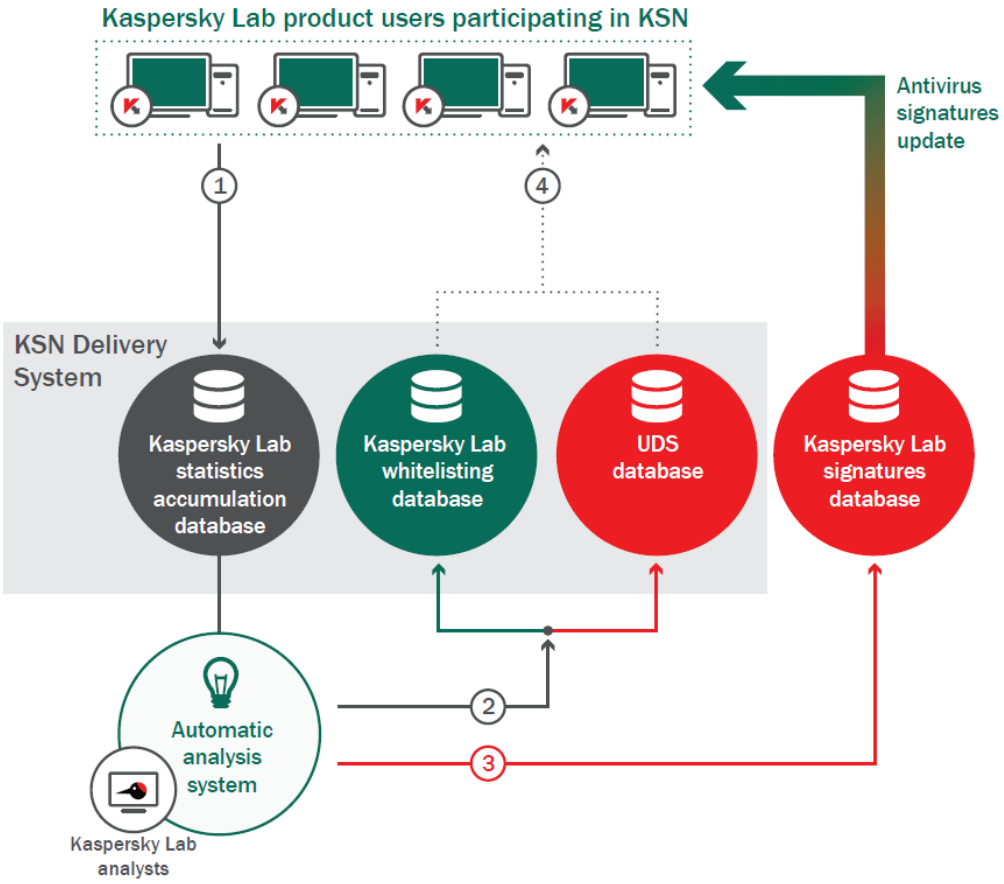
Wenn das Ausmaß der Gefahr, die ein Objekt darstellt, nicht bestimmt werden kann, werden die Daten an Experten von Kaspersky Lab gesendet. Dort wird eine zusätzliche, gründliche Analyse durchgeführt, bevor die Daten an das KSN gesendet wird, wo Gefahren direkt über die Cloud erkannt werden. Dieser Schritt ist besonders wichtig, da er dem KSN, wie auch jeder anderen Lösung von Kaspersky Lab, ermöglicht, lernfähige Systeme und menschliche Expertise zu vereinen.

Während es Stunden dauert, einen Eintrag in einer herkömmlichen Antivirus-Datenbank zu erstellen und hochzuladen, erhalten KSN-Nutzer innerhalb weniger Minuten nach Beginn eines Cyberangriffs einen entsprechenden Schutz. Durch eine kontinuierliche Aktualisierung der Liste legitimier Programme ist das KSN sowohl für Datenbanken als auch für die heuristischen Erkennung dienlich und unterstützt das Whitelisting sowie Technologien zur Programmkontrolle.

Eine weitere wichtige Funktion des KSN ist die Cloud-basierte Anti-Spam-Technologie. Hierbei werden Informationen aus der Cloud verwendet, um unerwünschte Nachrichten zu erkennen und zu blockieren, damit Nutzer keinen lokalen Anti-Spam-Filter benötigen.

Das untenstehende Flussdiagramm erläutert die grundlegenden Prinzipien, nach denen die Produkte von Kaspersky Lab mit dem KSN interagieren. Die Interaktion ist in fünf verschiedene Phasen aufgeteilt:

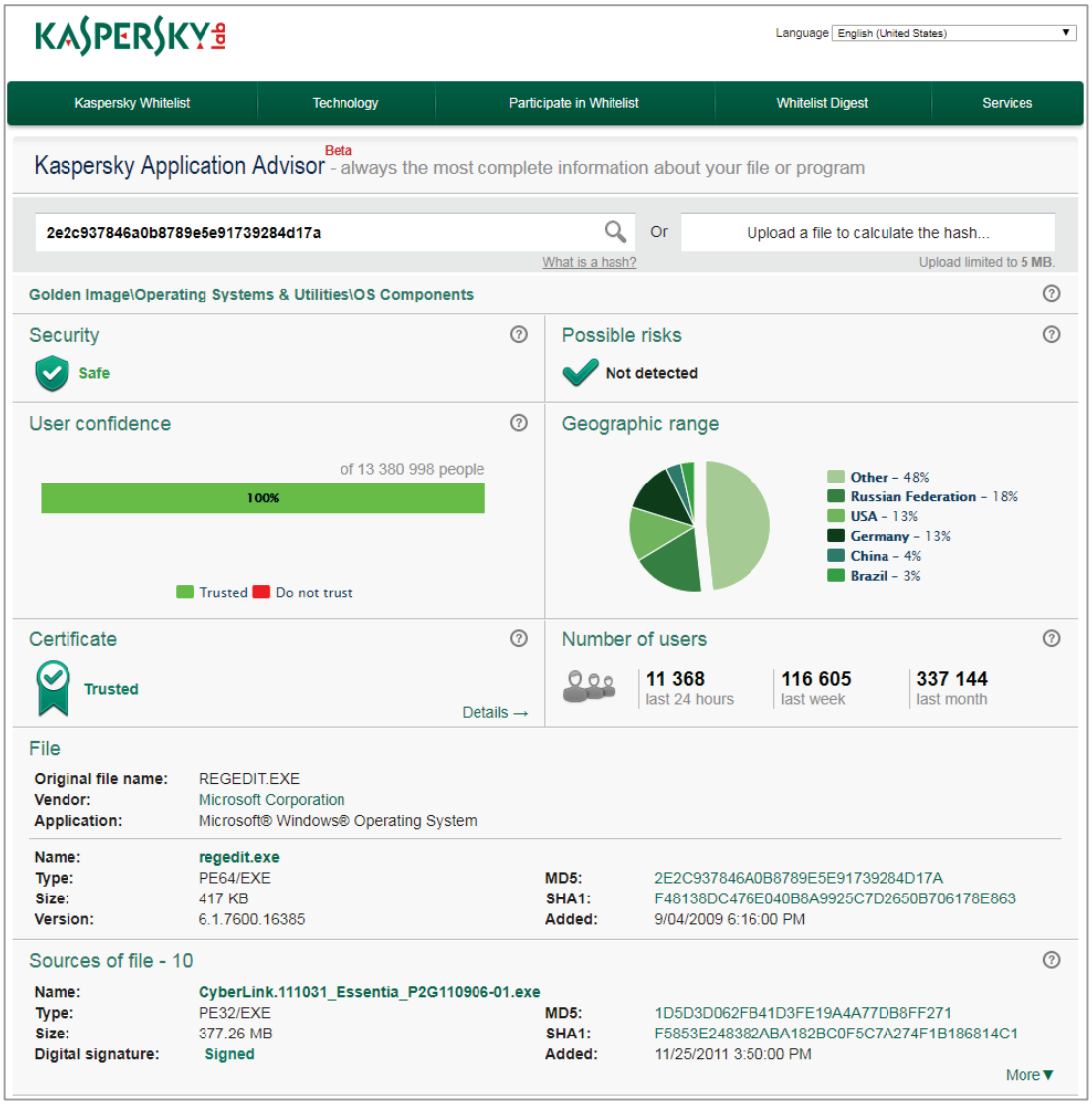
1. Das auf dem Gerät installierte Produkt erkennt verdächtige Aktivitäten am Standort, die nicht standardmäßig als gefährlich eingestuft werden, und sendet diese Informationen an die Cloud-Infrastruktur von Kaspersky Lab.
2. Wenn die Kaspersky-Nutzer einer bereits bekannten Cyberbedrohung begegnen (für die noch kein Eintrag in der Bedrohungsdatenbank besteht), sendet die Lösung eine Anfrage an das KSN und erhält eine sofortige Einschätzung. So wird ein optimaler Schutz gewährleistet.
3. Wenn die Datenbanken von Kaspersky Lab keinen entsprechenden Eintrag für eine beliebige Folge von Indikatoren vorweisen, werden die Daten an ein automatisches Analysesystem weitergeleitet, das die meisten neuen Cyberbedrohungen erkennt. Statt sich auf die Ressourcen von Nutzergeräten zu verlassen, beruft sich das System auf die leistungsfähigen personellen und maschinellen Ressourcen von Kaspersky Lab – die Informationen werden manuell von Kaspersky-Experten analysiert, wenn durch Big-Data-Analysen keine automatische Einschätzung erfolgen kann.
4. Wenn sich der Code oder die URL als schädlich herausstellt, werden die Informationen in der Datenbank des Urgent Detection System ergänzt und innerhalb weniger Minuten nach der Ersterkennung allen Nutzern zur Verfügung gestellt (und wenn die Lösung eine Anfrage an das KSN sendet, erfolgt eine sofortige Einschätzung zu dieser Bedrohung).
5. Erweisen sich Code oder URL als legitim, wird die Whitelisting-Datenbank entsprechend erweitert.



Die Front-End-Server des Kaspersky Security Network befinden sich in verschiedenen Ländern weltweit (Deutschland, Kanada, China usw.). Die Back-End-Server hingegen befinden sich in Russland; dort arbeitet der Großteil des Kaspersky-Forschungsteams für Malware-Schutz.

Kaspersky Security Network für Heimanwender

Abgesehen von den allgemeinen Vorteilen eines Cloud-basierter Schutzes, können Nutzer mit Verbraucherprodukten von Kaspersky Lab die Reputation sämtlicher Dateien oder Programme auf dem Gerät mithilfe von durch das Kaspersky Security Network bereitgestellten Daten prüfen. Diese Reputationstechnologie heißt „Kaspersky Application Advisor“:

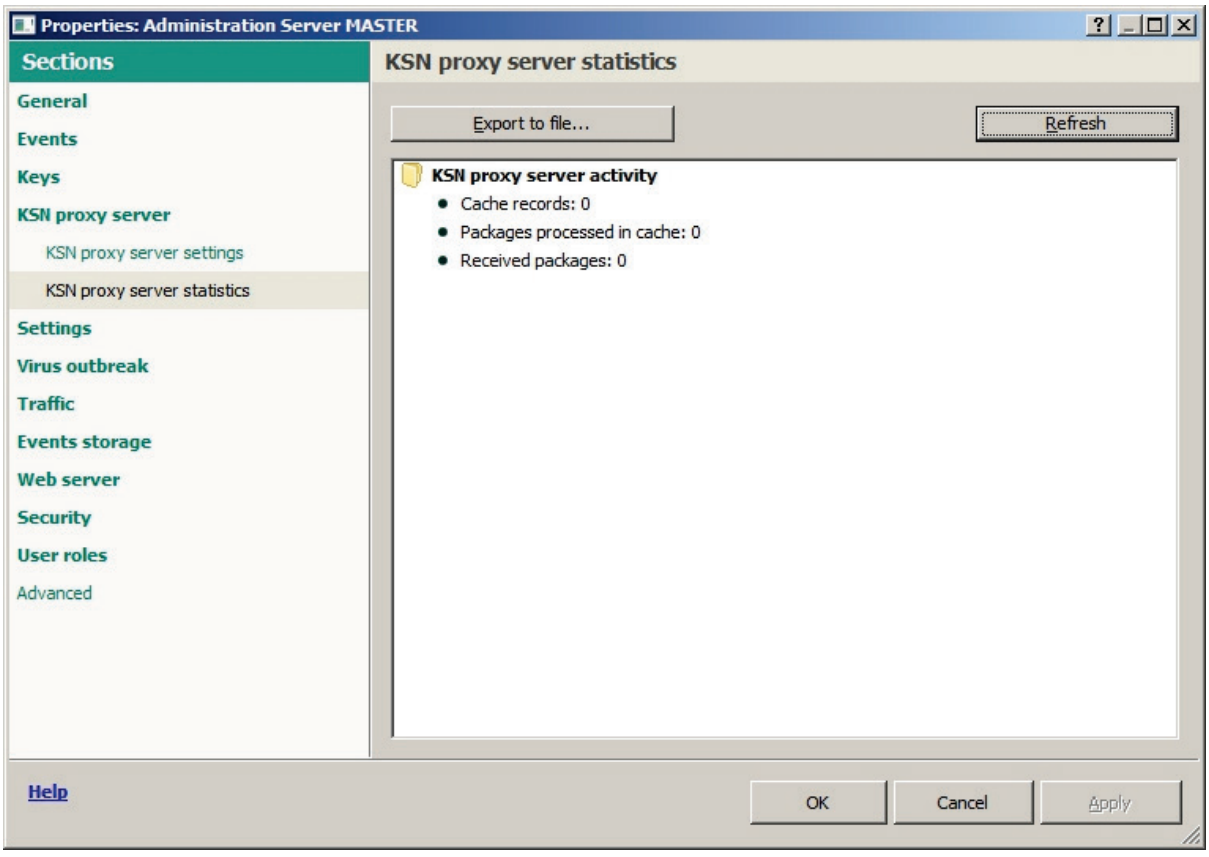


Eine solche Anfrage stellt eine Einschätzung der betreffenden Datei (Prüfung der Legitimität des Programms) sowie das Datum der erstmaligen Erstellung, die Beliebtheit nach Land und weitere Daten zur Verfügung. Mit dieser Funktion kann eine grundlegende Prüfung unbekannter Programme vor deren Start durchgeführt werden, obwohl dieselben Informationen automatisch erfasst werden, wenn ein Nutzer versucht, eine Datei zu öffnen.

Kaspersky Security Network für Unternehmen

Es gibt eine Reihe von Funktionen im Kaspersky Security Network, die speziell für Unternehmensprodukte ausgelegt sind. Vorrangig wird die Technologie des Cloud-basierten Schutzes für das Programm-Whitelisting unter Verwendung von Daten des Kaspersky Security Network herangezogen. Bekannte legitime Daten werden automatisch in Kategorien wie Spiele, kommerzielle Software usw. zusammengefasst. Mithilfe dieser Kategorien kann ein Systemadministrator unter Berücksichtigung der Sicherheitsrichtlinien schnell bestimmte Regeln für bestimmte Softwaretypen erstellen und anwenden. Die Daten für die Programm-Whitelisting-Datenbank werden von mehr als 600 führenden Softwareanbietern bereitgestellt und zusammen mit Informationen aus dem Crowdsourcing verwendet.

Die Verwaltungslösung des Kaspersky Security Center bietet Unternehmen eine fein abgestufte Kontrolle darüber, wie das Kaspersky Security Network Endpoints von Unternehmen schützt. Der Administrator kann wählen, ob der Cloud-basierte Schutz in den einzelnen Modulen von Kaspersky Endpoint Security for Business aktiviert oder deaktiviert sein soll. Ferner ist es möglich, die Datenübertragung an das Kaspersky Security Network zu deaktivieren. Um die Bandbreitennutzung zu verringern, kann ein interner Proxy für das Kaspersky Security Network innerhalb des lokalen Netzwerks für das Cachen von Daten des KSN installiert werden. IT-Abteilungen können bei Bedarf jederzeit den an das KSN übertragenen Datenverkehr überwachen:



Vorteile des Kaspersky Security Network

Heute wird die Technologie des Kaspersky Security Network auf Millionen Computern weltweit verwendet und zeichnet so ein detailliertes globales Bild über die Entwicklung und Verbreitung von Cyberbedrohungen, deren Quellen und die Anzahl der Infektionsversuche innerhalb eines bestimmten Zeitraums. Die vom Kaspersky Security Network durchgeführte weltweite Überwachung vereinfacht eine schnelle Reaktion auf neue Bedrohungen – ganz gleich, an welchem Standort sich Quellen und Ziele befinden.

Das Kaspersky Security Network bietet einen effizienten, zuverlässigen Schutz. Die Präzision wird durch einen eingespielten Interaktionsmechanismus zwischen Robotern und Experten gewährleistet – dem HuMachine-Prinzip von Kaspersky Lab. Dank dieser leistungsstarken Kombination werden mit dem KSN neue Bedrohungen identifiziert und blockiert, bevor diese sich verbreiten und erheblichen Schaden am IT-Netzwerk des Kunden anrichten können.

Dieses zuverlässige Abwehrsystem ist ein wesentlicher Bestandteil für die Sicherstellung eines stabilen, unterbrechungsfreien Betriebs von IT-Geräten und der Geschäftsprozesse, die dadurch unterstützt werden. Es ist für Unternehmen und Verbraucher, die von der Cybersicherheit der nächsten Generation profitieren möchten, nicht mehr wegzudenken.

[1] Der Inhalt hängt vom Produkt ab, nähere Informationen finden Sie im Abschnitt „Support“ der jeweiligen Webseiten von Kaspersky Lab.