Kaspersky®
Private Security
Network

Kaspersky Security Network: Sicherheit dank Big Data

Schutz vor jeder Generation von Bedrohung

Die Anzahl von Cyberangriffen nimmt täglich zu. Die Auswirkungen, beispielsweise wenn Daten gestohlen werden oder wichtige Informationen verloren gehen, betreffen Unternehmen jeder Größer - von Startups bis zum Großunternehmen.

Aber es geht nicht immer um die Anzahl von Angriffen: Täglich erscheinen neue Generationen von Malware, von denen viele neue, raffinierte Tricks anwenden, um bestehende Sicherheitslösungen zu umgehen. In dieser ständig neuen Umgebung ist Schutz nur so effektiv wie die Fähigkeit eines Anbieters, die Bedrohungslandschaft genauestens im Auge zu behalten und entsprechende Daten in praktisch umsetzbare Sicherheitsinformationen und neue Technologien zu übersetzen.

In dieser niemals enden wollenden Aufrüstung beider Seiten muss eine Lösung, die echte Cybersicherheit bieten will, effektiv auf neue Malware reagieren und gleichzeitig die nächsten Schritte von Cyberkriminellen vorausahnen. Eine wichtige Komponente dieser Fähigkeit ist die Nutzung von Cloud-Technologien, die verteilte Data-Mining- und Data-Science-Technologien anwenden, um die Bedrohungsinformationen zu verarbeiten. Die leistungsfähigeren Systeme, wie z. B. das Kaspersky Security Network, verfügen über global verbreitete Datenerfassungspunkte und leistungsstarke Big-Data-Verarbeitungseinrichtungen, um aus den rohen Daten letztlich ein höheres Maß an Schutz zu generieren. Doch auch menschliche Expertise ist ein wichtiger Aspekt dieser Verarbeitung. Sie ermöglicht eine hohe Erkennungsrate und somit das bestmögliche Ergebnis für den Benutzer.

Für die erfolgreiche Verwendung dieses Mechanismus sind drei wichtige Komponenten erforderlich:

- Erfassung globaler Statistiken zur Malware-Erkennung sowie Echtzeitdaten zu verdächtigen Aktivitäten
- Verarbeitung und Analyse von Big Data
- Schnelle Bereitstellung der Sicherheitsinformationen an Kunden

Der schwierigste Aspekt ist die Sortierung und Analyse der Daten. Bei der schieren Menge ist eine Data-Science-basierte Automatisierung erforderlich, um das eingehende Big-Data-Volumen zu verarbeiten. Doch auch menschliche Expertise ist und bleibt ein wichtiger Vorteil dieses Systems: Denn nur menschliche Intuition und Erfahrung können Maschinen dabei unterstützen, es mit den komplexen und oft äußerst erfinderischen Kreationen der Malware-Entwickler aufzunehmen. Die Kaspersky-Experten verfügen über Echtzeitzugriff auf alle erfassten Informationen, sodass sie wertvolle Einblicke in Bedrohungen gewinnen und dieses Wissen bei Untersuchungen sowie bei der Entwicklung neuer Erkennungstechnologien anwenden können. Zu den wichtigsten Vorteilen unseres Ansatzes zählen:

- Optimale Erkennung hoch entwickelter und zuvor unbekannter Malware
- Weniger Fehlalarme
- Deutliche Reduzierung der Reaktionszeiten bei neuen Bedrohungen – herkömmliche, signaturbasierte Reaktionen können Stunden benötigen, das KSN jedoch benötigt nur ca. 40 Sekunden.

Grundlegendes zum KSN

Durch die Nutzung von Echtzeitdaten, die freiwillig von Millionen von Endpoints weltweit bereitgestellt werden, unterliegt jede einzelne Datei, die die von Kaspersky Lab geschützten Systeme durchläuft, einer Analyse, die auf relevanten Bedrohungsinformationen beruht. Dieselben Daten stellen sicher, dass die am besten geeignete Gegenmaßnahme getroffen wird. Die Teilnahme am KSN erfolgt absolut freiwillig, und sämtliche erfassten Statistiken werden anonymisiert – es besteht also absolut keine Verbindung zwischen Daten und ihren tatsächlichen Benutzern. Ausführliche Informationen zu den erfassten Datentypen und zur Art der Datenübertragung finden Sie in der Endbenutzer-Lizenzvereinbarung (EULA).

KSN nutzt absolut sichere Verbindungen, um die Informationen zu übermitteln. Das System zur Datenübertragung entspricht den Branchenstandards. Sämtliche primäre Datenverarbeitung erfolgt automatisch, und der Zugriff ist nur in extremen Ausnahmefällen gestattet.

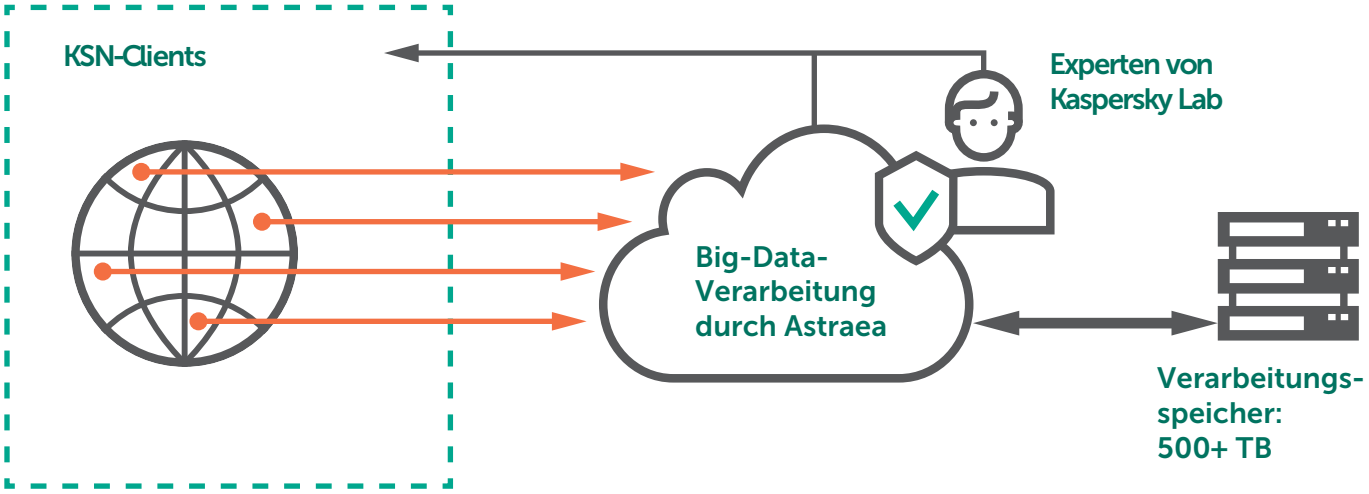

Abb. 1: Schema der Datenübertragung zwischen KSN-Elementen

Astraea – Smartes System mit Big-Data-Analyse

Pro Tag gehen im KSN Hunderte Millionen verschiedener Datensätze ein – eine unglaubliche Menge an Daten, die oft Hunderte Gigabyte täglich erreicht. Diese anonymisierten Daten werden komprimiert und für die künftige Verwendung gespeichert. Doch selbst nach ihrer Komprimierung sind noch Terabyte an Speicher notwendig.

Eines der Systeme, das das Kaspersky Security Network nutzt, um den enormen Datenstrom zu verarbeiten, nennt sich Astraea. Jeden Tag verarbeitet es Informationen zu Millionen von Objekten, sortiert und analysiert sie. Nach der Sortierung bewertet Astraea jedes Objekt, wobei nur dessen Metadaten, nicht aber seine Inhalte verwendet werden.

Jedes vom System erkannte verdächtige Ereignis wird anhand verschiedener Kriterien nach Wichtigkeit und potenzieller Gefahr eingestuft. Nach dieser Analyse wird die Reputation des Objekts berechnet, und es werden globale Statistiken zum Objekt angefordert. Was sagt die kollektive Intelligenz noch über das Objekt aus? Ist die Reputation in Wahrheit schlechter, als es eigentlich scheint? Oder handelt es sich um einen Fehlalarm? Durch diese Abfragen zusätzlicher Informationen kann das System eine präzisere Bewertung erstellen und so die Wahrscheinlichkeit von Fehlalarmen für andere Benutzer reduzieren.

Wenn die zusammengefassten Statistiken bestätigen, dass es sich um ein schädliches, sicheres oder unbekanntes Objekt handelt, wird diese Information ganz automatisch allen unterstützten Kaspersky-Produkten zur Verfügung gestellt, in denen die Benutzer das Kaspersky Security Network aktiviert haben.
Ähnlich verhält es sich mit der Verarbeitung schädlicher Webressourcen: Benutzer erhalten automatisch eine Warnung, wenn sie versuchen, entsprechende Ressourcen zu öffnen.

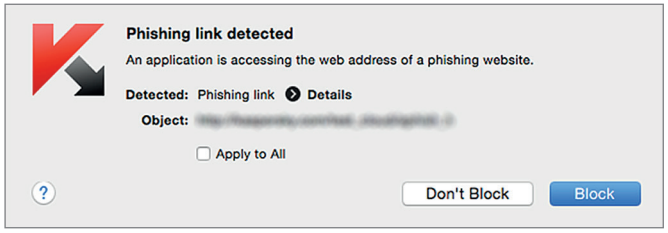

Abb. 2: Alarm zu gefährlicher Webseite

Doch trotz aller Vorteile der Automatisierung, ist echter Schutz ohne die Mitarbeit von Menschen unmöglich. Schließlich müssen die Systeme den Tricks und Umgehungstaktiken echter Cyberkrimineller standhalten. Deshalb verfolgt das KSN, wie auch andere Systeme von Kaspersky Lab, das HuMachine-Prinzip: die Verschmelzung der Leistungsfähigkeit von Maschinen mit der Erfahrung menschlicher Experten. Wie funktioniert es?

Wenn Sie das Ausmaß der Gefahr, die ein Objekt darstellt, nicht bestimmen können, werden die Daten an Experten gesendet. Diese führen eine zusätzliche, tief gehende Analyse durch, bevor sie die Daten an das KSN senden, wo Gefahren direkt über die Cloud erkannt werden. Gleichzeitig können die heuristischen Erkennungsmodelle so angepasst werden, dass sie viele verschiedene Malware-Exemplare erkennt, die auf ähnlichen Indikatoren basieren.

Astraea ist ein äußerst intelligentes System, das ständig dazulernt, um effektiv mit immer neuen Bedrohungen umgehen zu können. Die alten Lernkriterien werden jedoch zunehmend irrelevant. Stattdessen müssen neue Möglichkeiten gefunden und umgesetzt werden, um den Erfindungen der Gegenseite beizukommen. Hierfür benötigen die Maschinen die Hilfe menschlicher Experten.

Von den Experten in die Realität

Das KSN stellt Sicherheitsinformationen in Sekundenschnelle bereit. So wird in Echtzeit ein hohes Maß an Schutz vor realen Bedrohungen gewährleistet. Im Falle eines Massenangriffs, in dem die Malware-

Informationen bereits die KSN-Server, aber noch nicht die Erkennungsdatensätze der Endbenutzer erreicht haben, werden die entsprechenden Daten umgehend nach der Anfrage durch den Benutzer bereitgestellt.

Natürlich ist hierfür eine bestimmte Bandbreite erforderlich, und der Internetdatenverkehr wird eingeschränkt. Deshalb kann das KSN auf Caching-Server zurückgreifen, die im lokalen Netzwerk installiert sind, um die Auslastung der Internetverbindung zu reduzieren.

Wenn der Benutzer das KSN deaktiviert hat, erhält er nur bei Updates präzise Informationen zu neuer Malware. Zwischen den Updates wird der Schutz durch andere Mechanismen gewährleistet.

KPSN

Obwohl alle vom Kaspersky Security Network verarbeiteten Informationen vollständig anonymisiert werden und damit ihrem Ursprung nicht mehr zugeordnet werden können, ist sich Kaspersky Lab bewusst, dass für einige Unternehmen eine absolute Datensperre aufgrund behördlicher Auflagen oder interner Richtlinien unumgänglich ist. Bislang hatte dies zur Folge, dass diese Unternehmen auf cloud-basierte Sicherheitsdienste verzichten mussten.

Für diese Art von Kunden hat Kaspersky Lab nun ein eigenständiges Produkt entwickelt: Mit dem **Kaspersky Private Security Network** können Unternehmen fast alle Vorteile unserer weltweiten Cloud-basierten Bedrohungsinformationen nutzen, ohne dass dabei Daten ihren Sicherheitsperimeter verlassen. Es handelt sich also um die vollständig private, lokale Version des Kaspersky Security Network für ein einzelnes Unternehmen.

Das KPSN kann auf einem speziellen lokalen Server installiert werden und bietet so flexiblen Schutz für alle verbundenen Geräte. Es erfordert keine Internetverbindung: In besonders strengen Anwendungsumgebungen können Updates manuell über sichere Wechseldatenträger installiert werden. In beiden Fällen steigert die Bereitstellung eines eingehenden Datenstroms die Reaktionszeiten bei ständig neuen Bedrohungen deutlich:

Fazit

Die Notwendigkeit sofortigen Schutzes vor neuen Bedrohungen ist offensichtlich – selbst für Personen, die nicht direkt mit der Informationssicherheit zu tun haben. Selbst ohne die Aktivierung des Kaspersky Security Network bieten die verschiedenen Ebenen unserer Sicherheitstechnologien in unseren Lösungen effektiven Schutz für alle Benutzer.

Die sofortige, Cloud-basierte Sicherheit des KSN erweitert den Schutz jedoch um zusätzliche wichtige Mechanismen, die mithilfe von Echtzeitdaten zu Bedrohungen, autorisierten Anwendungen und anderen relevanten Informationen Fehlalarme reduzieren und die Erkennungsqualität steigern.

Aufgrund der Tatsache, dass komplexere zielgerichtete Bedrohungen mehr Schaden anrichten als Massen-Malware, kann der Wert der Sicherheitsinformationen aus dem Kaspersky Security Network nicht oft genug betont werden. Hierbei wird die höchstmögliche Präzision der Informationen durch die perfekte Interaktion zwischen Mensch und Maschine gewährleistet: Kaspersky HuMachine. Es ist für alle Unternehmen wichtig, in allen Situationen das bestmögliche Ergebnis zu erzielen. Das Kaspersky Security Network – oder seine private Version, das KPSN – unterstützen Unternehmen effektiv dabei, dieses Ziel zu erreichen.

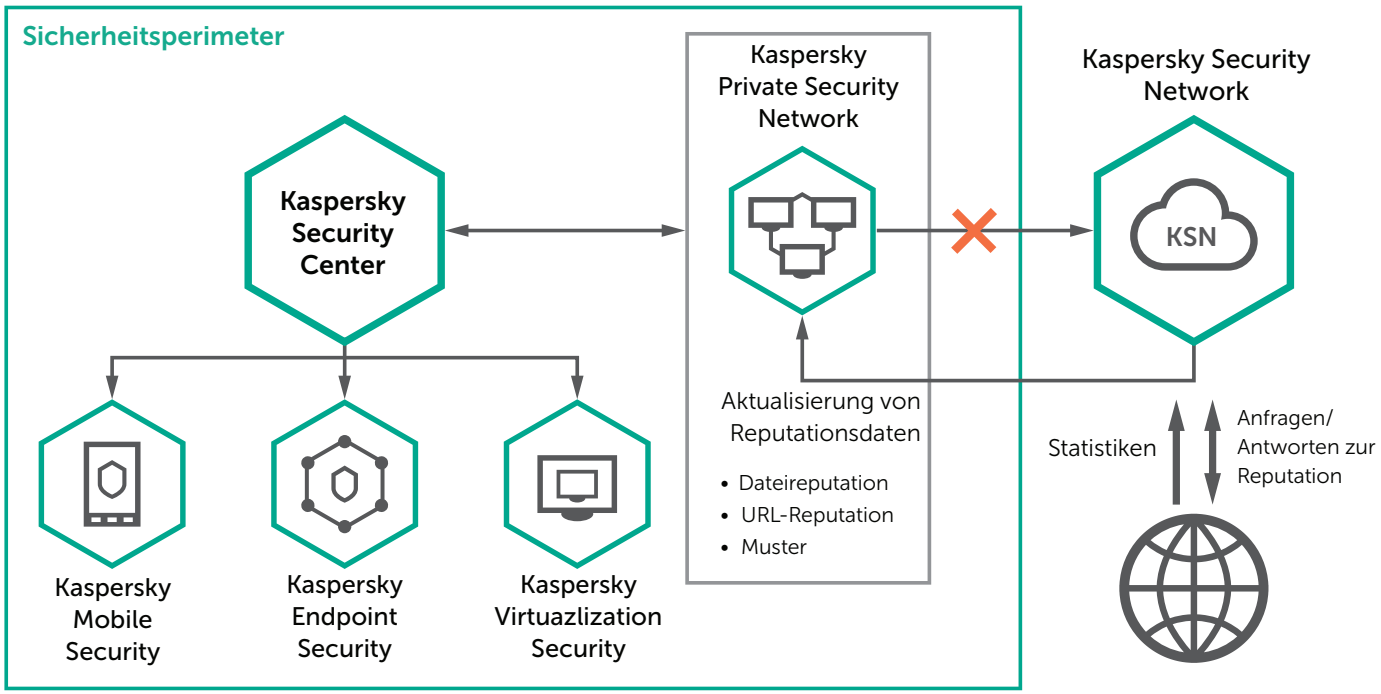

Abb. 3: Schema der KPSN-Infrastruktur im Sicherheitsperimeter

Informationen zur Internetsicherheit: **www.viruslist.de**
Informationen zu Partnern in Ihrer Nähe finden Sie hier:
https://www.kaspersky.de/partners

www.kaspersky.de
#truecybersecurity