KASPERSKY lab

KASPERSKY ANTI TARGETED ATTACK PLATFORM

Erkennung von hoch entwickelten Bedrohungen ... in Echtzeit

www.kaspersky.de

Die Anzahl von gezielten Angriffen auf Unternehmen nimmt zu – und die Techniken und Fertigkeiten der Angreifer sind höher entwickelt als jemals zuvor. Die gezielten Angriffe und hoch entwickelten Bedrohungen von heute sind schwerer zu erkennen und oft schwer einzudämmen und zu eliminieren. Aus diesem Grund benötigen Unternehmen eine umfassende, anpassungsfähige Sicherheitsstrategie.

Schwachstellen und moderne Bedrohungen

Die meisten Unternehmen haben bereits beträchtliche Investitionen in herkömmliche IT-Sicherheitslösungen getätigt, die sich häufig auf Gateway-Ebene befinden. Aber auch wenn diese präventiven Sicherheitstechnologien beim Schutz vor gängigen Bedrohungen, einschließlich Malware, Datenlecks, Netzwerkangriffen usw., sehr gute Dienste leisten, ist die Gesamtzahl der Sicherheitsvorfälle und -verletzungen in Unternehmen nicht zurückgegangen.

Hoch entwickelte, gezielte Bedrohungen können wochen-, monate- oder sogar jahrelang unbemerkt bleiben, während Cyberkriminelle wertvolle Informationen sammeln und/oder in wichtige Geschäftsabläufe eingreifen. Bei einem solchen Angriff entdecken präventionsbasierte Sicherheitstechnologien möglicherweise einige Vorfälle, versäumen es aber, festzustellen, dass diese einzelnen Vorfälle Teil eines weit gefährlicheren und komplexeren Angriffs sind, der dem Unternehmen beträchtlichen Schaden zufügen könnte und sich über einen längeren Zeitraum negativ auf das Unternehmen auswirken kann.

Gezielte Angriffe sind langfristige Verfahren, die die Sicherheit des Unternehmens gefährden und dem Angreifer unautorisierte Kontrolle über die IT des angegriffenen Unternehmens geben – außerdem helfen sie dem Angreifer, einer Erkennung durch herkömmliche Sicherheitstechnologien zu entgehen.

Für einige Angriffe werden hartnäckige Bedrohungen (Advanced Persistent Threats, APTs) verwendet, die zwar sehr effektiv, aber schwer implementierbar sein können. Für andere Angriffe wiederum wird unter Umständen nur ein einziges Verfahren angewendet, z. B. hoch entwickelte Malware oder Zero-Day-Attacken.

Zur Verbesserung des Sicherheitsniveaus, das von herkömmlichen Lösungen geboten wird, gehen viele Unternehmen dazu über, die Prozesse mithilfe von SIEM-Systemen (Security Information and Event Management) zu automatisieren. Einige Unternehmen gehen sogar soweit, dass sie ihre eigenen ihre eigenen Security Operations Center entwickeln – für die Korrelation von Ereignissen und Daten, Zentralisierung des Sicherheitsmanagements und Reaktion auf Vorfälle. Dieser Ansatz erfordert jedoch eine globale Sicht auf das Thema Sicherheit und ein fundiertes Fachwissen über die Analyse von Cyberbedrohungen, um die größte Wirkung zu erzielen. Selbst multinationale Konzerne sind selten in der Lage, die erforderlichen Experten für ihre internen Sicherheitsteams einzustellen, auszubilden und langfristig an das Unternehmen zu binden.

Überwindung der Grenzen präventiver Sicherheitstechnologien

Da die Ansätze von gestern, die nur auf Prävention beruhen, gegenüber gezielten Angriffen nicht effektiv sind, müssen Unternehmen ihre Sicherheit überdenken. Anderenfalls sehen sie sich der Gefahr ausgesetzt, dass nicht erkannt wird, wenn Cyberkriminelle Zugriff auf ihre Systeme erlangen.

Als international anerkannter Forscher auf dem Gebiet der Cyberbedrohungen unterstützt Kaspersky Lab eine Strategie, bei der Unternehmen einen kontinuierlichen, mehrstufigen Prozess zum Schutz vor gezielten Angriffen implementieren.

Die Ermittlung des Vorhandenseins eines gezielten Angriffs erfordert mehr als nur das Auffinden von schädlichen Codes oder unbefugten Verbindungen. Eine fortschrittliche Erkennung hängt von einem Verständnis des normalen Systemverhaltens und des normalen Benutzerverhaltens plus der konstanten Analyse aller Aktivitäten ab, um eine entsprechende Transparenz in der gesamten IT-Infrastruktur sicherzustellen. Um die neuesten Bedrohungen erkennen zu können, benötigen Unternehmen Updates über neue Angriffsmethoden und globale Bedrohungsexpertise.

Je mehr Zeit und Budget ein Unternehmen in die Sicherheit investiert, desto schwieriger ist es für Cyberkriminelle, in die Systeme dieses Unternehmens einzudringen. Als erster unerlässlicher Schritt muss das Unternehmen Schwachstellen in seinen aktuellen Systemen ermitteln und diese Probleme zeitnah beheben. Des Weiteren muss sichergestellt werden, dass sich Mitarbeiter über bestehende Sicherheitsrisiken bewusst sind, insbesondere da Cyberkriminelle sich das Potential des „menschlichen Versagens" zunutze machen und oft bei einem Angriff vorsätzlich auf Mitarbeiter abzielen. Darüber hinaus müssen die Sicherheitsbeauftragten eines Unternehmens in der Ermittlung und Priorisierung von Vorfällen geschult werden, die in Zusammenhang mit gezielten Angriffen stehen.

Anpassungsfähige Sicherheitsstrategie

Kaspersky Lab kann viele Erfolge bei der Aufdeckung von gezielten Angriffen und APTs in der Branche vorweisen. Nahezu ein Drittel der Mitarbeiter des Unternehmens besteht aus Experten im Bereich der Sicherheitsforschung und -analyse. Darüber hinaus empfängt das cloudbasierte Kaspersky Security Network (KSN) kontinuierlich Daten über neue Bedrohungen aus allen Teilen der Welt. Diese wichtigen Daten aus der Praxis unterstützen das Unternehmen bei der Erkennung von über 310.000 schädlichen Programmen und Bedrohungen tagtäglich.

Kaspersky Lab bietet Unternehmen Unterstützung bei der Änderung ihrer Sicherheitsstrategien zum Schutz vor hoch entwickelten Bedrohungen und gezielten Angriffen. Wir bieten eine einzigartige Kombination aus Technologien und Services, gestützt von wertvollen Sicherheitsdaten. So helfen wir Unternehmen dabei, gezielte Angriffe frühzeitig zu erkennen und die Risiken zu mindern, bevor größere Schäden verursacht werden.

Wir sind der Überzeugung, dass jedes Unternehmen eine anpassungsfähige Sicherheitsstrategie, die auf vier Grundpfeilern basiert, implementieren sollte:

- **VORHERSAGEN**: Unterstützung von Unternehmen zur Beurteilung ihrer aktuellen Sicherheit und Ermittlung von möglichen Angriffsmethoden zukünftiger gezielter Angriffe auf ihre Infrastruktur
- **REAGIEREN**: Unterstützung von Unternehmen bei der Ausführung von Untersuchungen und Schließung von Sicherheitslücken

- **VERHINDERN**: Blockierung von hoch entwickelten Bedrohungen und Verringerung der Gefahr von gezielten Angriffen
- **ERKENNEN**: Kontinuierliche Überwachung zur Ermittlung von Aktivitäten, die möglicherweise auf einen gezielten Angriff hinweisen

Die Kaspersky Anti Targeted Attack Platform erreicht äußerst hohe Erkennungsraten, da sie Echtzeit-Feeds basierend auf der neuesten Global Security Intelligence und globalen Bedrohungsinformationen vom Kaspersky Security Network erhält.

Bereitstellung einer mehrstufigen, anpassungsfähigen Sicherheitsstrategie

Die Kaspersky Anti Targeted Attack Platform ist Teil eines anpassungsfähigen, integrierten Ansatzes für die Unternehmenssicherheit. Eine Echtzeitüberwachung des Netzwerkverkehrs, kombiniert mit Objekt-Sandbox und Endpoint-Verhaltensanalyse, bietet einen detaillierten Einblick in die Vorgänge der IT-Infrastruktur eines Unternehmens. Der Ansatz einer anpassungsfähigen Sicherheitsstrategie schützt Unternehmen vor hoch entwickelten Bedrohungen, gezielten Angriffen, neuer Malware, einschließlich Ransomware und Crimeware, sowie hartnäckigen Bedrohungen (Advanced Persistent Threats, APTs).

Durch die Korrelation von mehrstufigen Ereignissen, einschließlich Netzwerk, Endpoints und globale Bedrohungslage, bietet die Kaspersky Anti Targeted Attack Platform die Erkennung von komplexen Bedrohungen nahezu in Echtzeit und ermöglicht retrospektive Untersuchungen.

ANALYSE VON VERDÄCHTIGEN OBJEKTNUTZLASTEN UND APT-ENTDECKUNG

Für die mehrstufige Analyse von Objekten ist im Lieferumfang der Kaspersky Anti Targeted Attack Platform Folgendes enthalten:

- Netzwerksensoren zur Überwachung des Netzwerkverkehrs für die Erkennung von Indikatoren von Cyberangriffen
- E-Mail-Sensoren zur Ausschleusung von potentiell schädlichen Objekten aus E-Mail-Anhängen
- Websensoren zur Ausschleusung von Objekten aus dem Webverkehr unter Verwendung des ICAP-Protokolls
- Advanced-Sandbox-Technologie, die eine isolierte, virtualisierte Umgebung bereitstellt, in der verdächtige Objekte von Netzwerk-, E-Mail- und Websensoren sowie die Artefakte, die sie erzeugen, dynamisch untersucht werden können
- Die Daten von den Netzwerk- und Endpoint-Sensoren werden dann vom Targeted Attack Analyzer kombiniert und mit der „Baseline" verglichen, um verdächtige Aktivitäten aufzuspüren und das Sicherheitsteam darüber durch präzise Alarmmeldungen zeitnah zu informieren.

Die Advanced Sandbox ist mit zahlreichen Technologien ausgestattet, die verhindern, dass die Malware erkennt, dass sie in einer Sandbox ausgeführt wird. Dadurch kann sich die Malware nicht automatisch deaktivieren und die Preisgabe von Daten über ihre Aktivitäten verhindern.

ÜBERWACHUNG VON UNGEWÖHNLICHEM UND VERDÄCHTIGEM VERHALTEN

Für die fortschrittliche Netzwerkverhaltensanalyse ist im Lieferumfang der Kaspersky Anti Targeted Attack Platform Folgendes enthalten:

- Endpoint-Sensoren (Light Agents) zur Sammlung von Informationen über netzwerkaktive Prozesse, die auf den Endpoints des Unternehmens ausgeführt werden
- Netzwerksensoren zum Abfangen von rohem IP-Verkehr und Internetaktivitäten, um Metadaten auszuschleusen
- Targeted Attack Analyzer, der ein Verständnis für normale Verhaltensmuster erzeugt und anschließend durch die Überwachung von Netzwerksensor-Metadaten und Daten, die von den Endpoint-Sensoren empfangen werden, ungewöhnliches und abweichendes Verhalten im Unternehmensnetzwerk erkennen kann

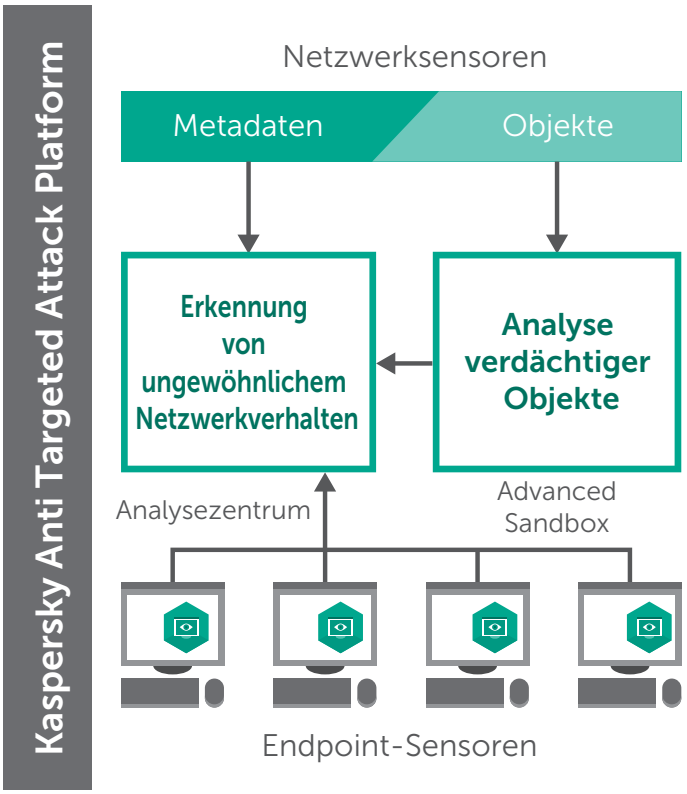
EINFACHE BEDIENUNG UND VERWALTUNG

Der Targeted Attack Analyzer empfängt Daten von den Netzwerk- und Endpoint-Sensoren, analysiert diese umfassend und liefert Ergebnisse zur Bedrohungserkennung. Alle Ergebnisse zur Bedrohungserkennung werden zur Verwendung für Ermittlungen nach dem Angriff gespeichert.

Ein Dashboard mit komfortabler Ausgabefilterung bietet auf einen Blick detaillierte Informationen über Aktivitäten und potentielle Probleme, um Unternehmen bei der frühzeitigen Erkennung von Sicherheitsvorfällen zu unterstützen. Darüber hinaus werden auf der Kaspersky Anti Targeted Attack Platform detaillierte Protokolle über Warnungen für die Analyse zur Unterstützung von Vorfallreaktionen und Untersuchungen nach dem Angriff aufgezeichnet. Vorfallprotokolle können auch an das SIEM-System des Kunden weitergeleitet werden.

VORFALLREAKTIONSDIENST BEI GEZIELTEN ANGRIFFEN

Wenn die Kaspersky Anti Targeted Attack Platform feststellt, dass ein Unternehmen angegriffen wird, bieten die Sicherheitsexperten von Kaspersky Lab einen umfassenden Vorfallreaktionsdienst, um den Angriff zu analysieren und bei der Verwaltung der Kosten für Korrekturmaßnahmen Unterstützung zu leisten. Der Vorfallreaktionsdienst deckt alles von einem ersten Assessment des Vorfalls über die Beweissammlung und forensische Analyse bis hin zur Einreichung eines detaillierten Untersuchungsberichts und Schadensregulierungsplans ab.



DIENST FÜR DIE ERKENNUNG GEZIELTER ANGRIFFE

Da Kaspersky Lab sich bewusst ist, dass manchmal auch kleine Unternehmen Ziel von Angriffen sein können, die über einen sehr langen Zeitraum hinweg aktiv bleiben können und relativ schwer erkennbar sind, bietet das Unternehmen einen eigenen Dienst für die Erkennung gezielter Angriffe. Dieser Dienst umfasst eine Prüfung, bei der Sie nicht verpflichtet sind, Produkte zur Erkennung gezielter Angriffe zu kaufen.

Zusätzlich bieten Sicherheitsexperten von Kaspersky Lab Penetrationstests, Assessments der Programmsicherheit und Cybersicherheits-Schulungsdienste, um Unternehmen besser auf den Schutz vor künftigen Angriffen vorzubereiten.

Kaspersky Anti Targeted Attack Platform/Jan 2016/Global

KASPERSKY lab