KASPERSKY lab

Hochentwickelter Schutz und Threat Intelligence zur Minderung des Risikos gezielter Angriffe

Kaspersky Threat Management and Defense

www.kaspersky.de
#truecybersecurity

Das zunehmende Risiko durch komplexe Bedrohungen und zielgerichtete Angriffe

Die Wiederherstellung eine Woche nach der Entdeckung eines Vorfalls 200% mehr, verglichen mit einer sofortigen Reaktion.*

* Ergebnisse der Umfrage zu globalen Unternehmens-IT-Sicherheitsrisiken, die von Kaspersky Lab 2016 weltweit durchgeführt wurde

15 % der Unternehmen sind bereits Opfer eines gezielten Angriffs geworden; von diesen haben mehr als 53 % vertrauliche Daten durch einen solchen Angriff verloren.*

*Bericht von Kaspersky Lab zu globalen IT-Risiken 2015

Jedes Unternehmen, das groß genug ist, um eine wichtige Position in seinem Markt einzunehmen, stellt ein potentielles Ziel dar. Das bedeutet aber nicht, dass kleinere Unternehmen immun sind – in vielen Fällen werden sie von Kriminellen als leichtes Opfer angesehen, das quasi als Sprungbrett dient, von dem aus größere Ziele erreicht werden können. Doch wenn es um Marktführer geht, steigen die Chancen, Opfer eines solchen Angriffs zu werden, erheblich. Die Frage lautet nicht „ob", sondern „wann" ...

Von wem werden Angriffe ausgeführt?

Cyberkriminelle – die Daten an den höchsten Bieter verkaufen oder einfach Geld stehlen. Sie entwickeln ihre Cybertools normalerweise selbst oder kaufen sie im Dark Web.

Mitbewerber – auf der Suche nach vertraulichen Daten oder gar Möglichkeiten, Sabotage zu betreiben. Sie erkaufen sich für gewöhnlich die Dienste von Cybersöldnern.

Cybersöldner – Meister der Cyberspionage, sie entwickeln ihre eigenen Tools und verkaufen ihre „Dienste" an den höchsten Bieter.

Hacktivisten – geben vor, für das „Gemeinwohl" zu arbeiten, sind erfinderisch, nutzen komplexe Toolsets und stellen ein ernsthaftes Problem für alle Organisationen dar, die ihre Aufmerksamkeit erregen.

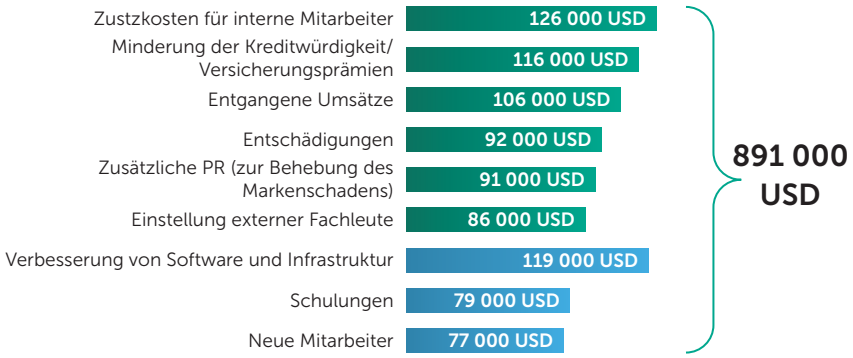
Staatliche Stellen – sie können dies bestreiten, aber es ist allgemein bekannt, dass Regierungen überall auf der Welt regelmäßig Einzelpersonen, Gruppen und Unternehmen überwachen. Ihre Toolsets können hochkomplex, kostspielig und schwer zu erkennen sein.

Bedrohungslage für Unternehmen

Zielgerichtete Angriffe und komplexe Bedrohungen, darunter hoch entwickelte, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs), stellen eine der größten Gefahren für Unternehmenssysteme dar. Obwohl sich Bedrohungen – und die Techniken, die Cyberkriminelle nutzen – ständig weiterentwickeln, verlassen sich noch zu viele Organisationen auf überholte Denkweisen und Sicherheitstechnologien von gestern, um sich vor den Bedrohungen von heute und morgen zu schützen.

Hoch entwickelte, zielgerichtete Bedrohungen können wochen-, monatelang oder sogar jahrelang unentdeckt bleiben, während ihre Akteure langsam und unbemerkt Informationen sammeln und schrittweise daran arbeiten, die individuellen Schwachstellen in den Systemen ihrer gewählten Ziele auszunutzen. Anders als reguläre Malware werden hoch entwickelte, gezielte Bedrohungen aktiv durch die Täter gesteuert und verwaltet. Das Ziel geht dabei über die Verbreitung von Malware hinaus, denn der Plan ist, innerhalb der Unternehmensgrenzen zu unentdeckt zu bleiben. Diese Angriffe sind das Ergebnis einer häufig akribischen Recherche durch geduldige Akteure, die bereit sind zu warten, bis ihr Ziel erreicht ist.

Durchschnittliche Verluste durch einen einzelnen gezielten Angriff:



Interne und externe Faktoren für eine erfolgreiche Sicherheitsverletzung

Schlüsselfaktoren für die erfolgreiche Entwicklung gezielter Angriffe auf IT-Infrastrukturen sind unter anderem:

- versteckte und Schatten-IT
- unkontrollierte Konnektivität von IoT-Geräten
- unternehmenskritische Abhängigkeit von der Digitalisierung
- fehlende Präventivfähigkeiten und eine zu optimistische Einschätzung der aktuellen Perimeter-Sicherheit
- geringes Bewusstsein der Mitarbeiter für Informationssicherheitsrisiken
- mangelnder Einblick in die IT-Umgebung und insbesondere in das Netzwerk-Routing
- proprietäre bzw. veraltete Software und Betriebssysteme
- mangelnde Qualifikation des Sicherheitsteams in Bezug auf Malware-Forschung, digitale Forensik, Vorfallsreaktion und Threat Intelligence

Welche Risiken bestehen?

Risiken für alle Organisationen:

- Nicht autorisierte Transaktionen
- Diebstahl oder Beschädigung kritischer Daten
- Geheime Manipulation von Prozessen
- Untergrabung durch Wettbewerber
- Erpressung
- Identitätsdiebstahl

Risiken für wichtige Industriezweige:

Finanzdienstleistungen

- Nicht autorisierte Transaktionen
- Angriffe auf Geldautomaten mit Bargeld-Diebstahl
- Identitätsdiebstahl

Behörden

- Datenmanipulation
- Spionage
- Beschränkte Verfügbarkeit von Onlinediensten
- Identitätsdiebstahl
- Hacktivismus

Fertigung und Hightech

- Spionage (Know-how)
- Beeinträchtigung kritischer Technologieprozesse

Telekommunikation

- Angriffe auf Unternehmenskunden mithilfe der Telekommunikations-Infrastruktur
- Manipulation von E-Mail-Servern für Social Engineering
- Kontrolle über das Abrechnungssystem
- Manipulation von Webressourcen für Phishing-Zwecke
- Nutzung kompromittierter Infrastruktur (Geräte/IoT) für DDoS-Angriffe

Energie- und Versorgungsunternehmen

- Manipulationen mit Berechnungsdaten
- Angriffe auf Technologienetzwerke mit physischen Schäden

Massenmedien

- Hacktivismus
- Kompromittierte Websites (Verunstaltung, Phishing) und Verbreitung von Angriffen unter einem Massenpublikum

Gesundheitswesen

- Diebstahl von Patienteninformationen
- Angriffe auf Telemedizinausrüstung

Zielgerichtete Angriffe – Cyberkriminalität als Berufsfeld

Die meisten zielgerichteten Angriffe werden von erfahrenen Cyberkriminellen und Hackern überwacht, die damit vertraut sind, jede Phase ihres Angriffs anzupassen, um herkömmliche Abwehrmaßnahmen zu überwinden, Schwachstellen auszunutzen und den Wert der Ressourcen, die sie stehlen können, zu maximieren – finanzielle Mittel, vertrauliche Daten und vieles mehr eingeschlossen.

Die einst als Computerfreaks abgestempelten Angreifer haben sich in Profis verwandelt, für die Cyberkriminalität ein Geschäft ist. Ihre einzige Motivation, ein Unternehmen gezielt anzugreifen, ist der maximale Gewinn, der bereits vor dem Angriff auf Grundlage der damit verbundenen Kosten und der potentiellen Gewinne berechnet wird. Das Ziel besteht natürlich darin, die Vorlaufkosten zu minimieren, indem der Angriff so billig wie möglich und mit maximalen finanziellen Ergebnissen erfolgt.

Die meisten zielgerichteten Angriffe basieren auf einer Kombination aus Social Engineering und einem speziell angepassten Toolset. Die Kosten für die Durchführung eines wirksamen gezielten Angriffs sind deutlich gesunken, wodurch die Gesamtzahl der Angriffe weltweit entsprechend gestiegen ist.

Was steht also auf dem Spiel, wenn eine Organisation wie die Ihre einem gezielten Angriff zum Opfer fällt?

Direkte Schäden	Ausgaben für Reaktion
Beseitigung + Entgangene Umsätze + Ausfallzeiten	Systeme + Stellenbesetzung + Schulungen
	zur Verhinderung weiterer Verletzungen

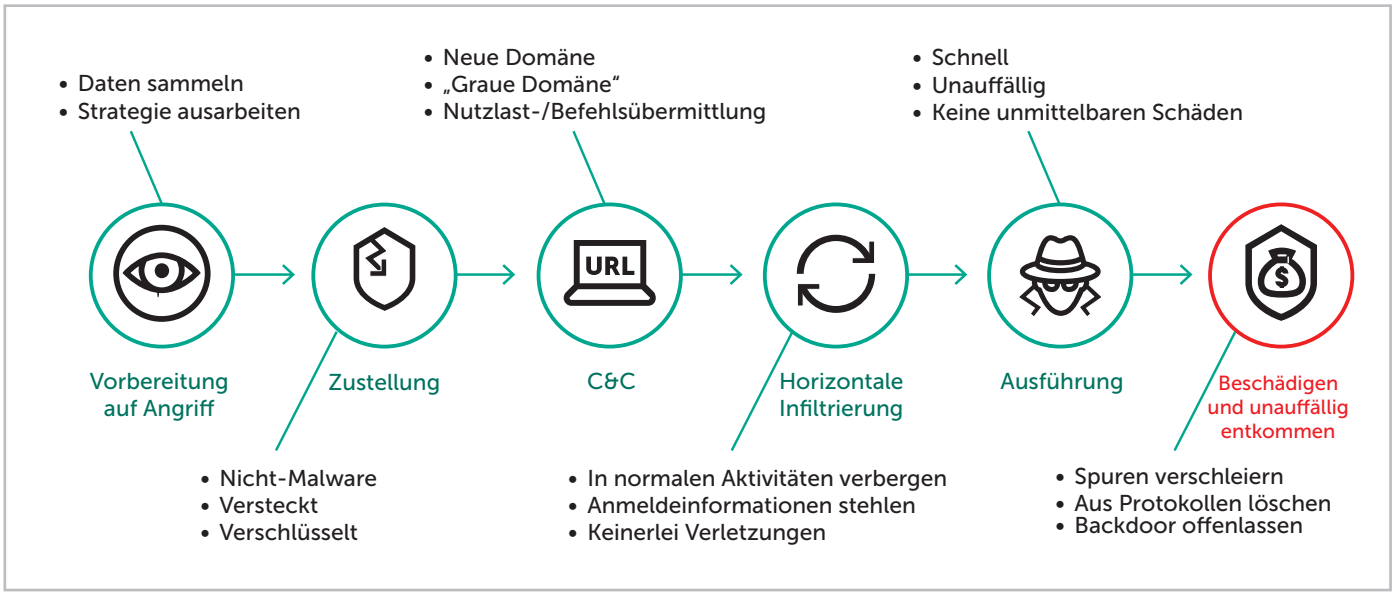
Unmittelbare finanzielle Verluste: Angreifer können Cyberfinanzbetrug betreiben, indem sie Zugangsdaten für Bankkonten stehlen, um auf die Unternehmenskonten zuzugreifen und betrügerische Transaktionen durchzuführen.

Störung wichtiger betrieblicher Abläufe: Während einige Angreifer als bloße Nebenerscheinung kritische Geschäftsprozesse behindern oder verlangsamen, geht es anderen um deren vorsätzliche Sabotage. Selbst wenn ein Angriff erkannt wird, werden die Störungen noch über einen gewissen Zeitraum andauern, in dem das betroffene Unternehmen Untersuchungen durchführt und die Betriebsabläufe wiederherstellt, was zum Verlust weiterer Geschäftschancen führen kann.

Wiederherstellungskosten: Nach einem Angriff können Sie mit hohen Kosten konfrontiert werden, die in ihrem Budget nicht vorgesehen waren. Durch das Wiederherstellen von Systemen und Prozessen fallen sowohl Investitionskosten als auch Betriebsausgaben an – z. B. durch die Beauftragung von Sicherheits- und Systemberatern.

Anatomie eines gezielten Angriffs

Theoretisch wirkt die Kill Chain eines zielgerichteten Angriffs ziemlich simpel: Erkundung und Tests, Eindringen, Verbreitung, Ausführung, Ergebnis. Das kann zur Annahme führen, dass durch das automatische Blockieren der ersten Schritte eines mehrstufigen Angriffs der Angriff selbst vereitelt werden kann.



In Wirklichkeit jedoch sind zielgerichtete Angriffe in Bezug auf ihr Voranschreiten wie auch ihre Ausführung sehr fortschrittlich und nichtlinear. Daher sollten automatisierte Erkennungsfunktionen, unterbrechungsfreie Überwachung und Threat Hunting Teil einer mehrstufigen Verteidigungsstrategie sein.

Gezielte Angriffe sind langfristige Verfahren, die die Sicherheit des Unternehmens gefährden und dem Angreifer unautorisierte Kontrolle über die IT des angegriffenen Unternehmens geben. Sie helfen 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 wiederum wird unter Umständen nur ein einziges Verfahren angewendet, z. B. hoch entwickelte Malware oder Zero-Day-Exploits.

Ein zielgerichteter Angriff ist ein langwieriger Prozess, der die Sicherheit verletzt und Cyberkriminellen ermöglicht, Autorisierungsverfahren zu umgehen und mit der IT-Infrastruktur zu interagieren, ohne auf herkömmliche Weise entdeckt werden zu können.

Somit handelt es sich allem voran um einen IT-first-Prozess – also um eine fortlaufende Aktivität im Sinne eines Projekts und nicht um eine einmalige böswillige Aktion. Nach unserer Erfahrung bei der Überwachung globaler Angriffe dauern solche Operationen in der Regel mindestens 100 Tage, bei Behörden, großen Marktteilnehmern und kritischen Infrastrukturen mitunter sogar Jahre.

Zudem zielt der Prozess auf eine bestimmte Infrastruktur, ist auf die Überwindung spezifischer Sicherheitsmechanismen ausgerichtet und kann anfangs auch die gezielte Ansprache von Mitarbeitern mit deren Namen per E-Mail oder Social Media beinhalten. Das ist ein völlig anderer Ansatz als bei den Massen-E-Mails von Angreifern, die Standard-Malware nutzen und ganz andere Ziele verfolgen. Im Falle eines zielgerichteten Angriffs sind die Methodik und die Phasen der Kill Chain auf das spezifische Opfer zugeschnitten.

Und schließlich wird der Vorgang normalerweise von einer organisierten Gruppe oder einem Team von Profis geleitet, das manchmal auf internationaler Ebene agiert und mit ausgeklügelten technischen Tools ausgestattet ist. Man sogar so weit gehen und die Aktivitäten dieser Cyberkriminellen nicht nur als Projekt bezeichnen, sondern eher als eine Operation mit mehreren Kampfeinsätzen. Angreifer stellen beispielsweise typischerweise eine Liste von Mitarbeitern zusammen, die potentiell als „Gateway“ zur Zielorganisation und deren Netzwerke dienen können, und analysieren die Onlineprofile und Social-Media-Aktivitäten dieser Mitarbeiter. Danach ist die Aufgabe, die Kontrolle über den Arbeitsrechner des Opfers zu erlangen, mehr oder weniger gelöst. Wenn der Computer des Mitarbeiters infiziert ist, übernehmen Eindringlinge die Kontrolle über das Netzwerk, von wo aus sie ihre kriminellen Aktivitäten steuern können.

Herausforderungen für die Unternehmenssicherheit

Da das Risiko komplexer Bedrohungen exponentiell zunimmt, implementieren viele Unternehmen bereits Technologien und Services – in der Hoffnung, eine höhere Stufe der Transparenz und des Schutzes vor aktuellen Bedrohungen zu erreichen. Doch ohne einen mehrschichtigen Ansatz und strategische Planung bleiben diese Bemühungen unter Umständen hinter den Erwartungen zurück.

Die enttäuschenden Ergebnisse von „Patchwork"- oder unstrukturierten Sicherheitsinvestitionen sind dann etwa:

1. größere Investitionen in eine Sandbox, in eigenständige Technologien oder in den Aufbau eines SOC, von denen keine die entsprechenden Sicherheitsverbesserungen bringt.

Perimeter-Sicherheitstechniken wie Firewalls und Anti-Malware-Software können sich gegen opportunistischere Angriffe behaupten. Anders verhält es sich hingegen bei gezielten Angriffen.

Einige Anbieter sind den Weg gegangen, mit einer breiten Palette an eigenständigen, individuellen Produkten auf APTs zu reagieren. Zu diesen Produkten zählen Sandboxes, Netzwerkanomalie-Analysen oder sogar Endpoint-fokussierte Überwachung. Während diese Elemente im Einzelnen Schutz bieten und Toolsets von Cyberkriminellen sowohl theoretisch als auch praktisch blockieren, sind sie für sich genommen nicht ausreichend, um einen gezielten koordinierten Angriff abzuwehren.

Um das zu erreichen, ist die Erkennung von mehreren Vorfällen erforderlich, die auf allen Ebenen einer Unternehmensinfrastruktur auftreten. Die gewonnenen Informationen können dann mit einem mehrschichtigen Analysesystem verarbeitet werden, gefolgt von der Interpretation mithilfe von Echtzeit-Security-Intelligence aus einer vertrauenswürdigen Quelle. Mit anderen Worten: Ihre optimale Investition ist ein Ansatz, der das Beste aus mehreren Technologien integriert, einschließlich Sandboxing mit der Analyse von Netzwerkanomalien und Endpoint-Ereignissen in einem übergreifenden End-to-End-Prozess.

2. Aktuelle Lösungen generieren zu viele Sicherheitsvorfälle für Ihr SOC-Team, um sie innerhalb eines vernünftigen Zeitrahmens verarbeiten, analysieren, priorisieren und darauf reagieren zu können.
3. Sicherheitskompetenz, die dem aktuellen Entwicklungsstand der Bedrohungen nicht entspricht. Sicherheitsexperten sind zwar in der Erkennung von Vorfällen und in der schnellen Abwehr von Verletzungen (Golden Image, Blacklisting von URLs/Dateien, Erstellung einiger Regeln) geschult, aber nicht vollständig dafür qualifiziert, einen umfassenden Reaktionsprozess zu implementieren (Bestimmung von Risikostufen, Durchführung von Erstanalysen, Untersuchung, Eindämmung, Forensik).
4. Unzureichender Einblick in den Betrieb. Während eines zielgerichteten Angriffs können Cyberkriminelle herkömmliche Sicherheitslösungen leicht umgehen, indem sie gestohlene Anmeldedaten und legale Software verwenden, sodass sie scheinbar keine Systemverletzungen verursachen.

Da Angreifer alles daransetzen, ihre schädlichen Aktivitäten zu verbergen, kann es für das interne IT-Sicherheitsteam sehr schwierig sein, einen Angriff auszumachen. Und das bedeutet, dass die Angreifer über einen längeren Zeitraum Schaden anrichten können.

Tatsächlich ist Malware für nur 40 % der Sicherheitsverletzungen verantwortlich. Wie wir gesehen haben, werden von Angreifern jedoch verschiedene Techniken für den Zugriff auf Unternehmenssysteme eingesetzt.
Und selbst dann, wenn Malware verwendet wird, sind 70 bis 90 % davon speziell für das Unternehmen entwickelt, in dem die Malware entdeckt wird (Verizon: Data Breach Investigation Report).

5. Probleme beim Bestimmen der intern einzusetzenden und auszubauenden Fachkenntnisse und der auszulagernden Sicherheitsaufgaben sowie der Aufgaben, die gefahrlos automatisierten Systemen überlassen werden können.

Angesichts der zunehmenden Schwere von Sicherheitsvorfällen und ihrer potentiellen Auswirkungen auf die Gesamteffektivität des Unternehmens besteht eine der größten Herausforderungen für die Sicherheitsabteilung darin, eine ausreichende Anzahl und ein ausreichendes Angebot an entsprechend qualifizierten Experten bereitzustellen. Eine vollständig wirksame Sicherheitsstrategie erfordert nicht nur unterbrechungsfreie Überwachungs- und Erkennungsfunktionen, sondern auch eine schnelle Reaktion und eine qualifizierte Abwehr mit entsprechenden forensischen Prozessen.

Herkömmliche SOC-Teams konzentrieren sich in der Regel nur auf einen Teil dieser Aufgabe, nämlich Erkennung und Reaktion. Der Einsatz automatisierter Lösungen hilft, Experten für die nächsten Schritte im Incident-Management-Prozess zu entlasten, doch nur wenige Unternehmen sind bereit, jede komplexe Aufgabe intern zu erledigen. Die Herausforderung besteht also darin, zu bestimmen, welche Aspekte des Gesamtprozesses vom internen Team übernommen werden sollten (Verwaltung, Risikoqualifizierung, Priorisierung, schnelle Wiederherstellung) und welche besser an Spezialisten ausgelagert werden (Malware-Forschung, digitale Forensik, Vorfallsreaktion, Threat Hunting) .

Sandboxes

Viele Lösungen zur Erkennung gezielter Angriffe auf dem Markt bestehen lediglich aus einer eigenständigen Sandbox. Sogar Anbieter, die keine aktuellen Erfolge bei der Erkennung neuer, hoch entwickelter Bedrohungen vorweisen können, geben vor, Sandboxes anzubieten, die häufig nicht viel mehr als eine Erweiterung ihrer Anti-Malware-Engines darstellen – ohne nennenswerte Threat Intelligence dahinter.

Die fortschrittliche Sandbox von Kaspersky Lab stellt nur einen weiteren Bestandteil unserer integrierten Erkennungsfunktionen dar. Sie wurde direkt aus unserem laboreigenen Sandbox-Komplex entwickelt, der Technologie, die wir seit mehr als einem Jahrzehnt einsetzen. Ihr Funktionsumfang wurde auf Grundlage der Statistiken zur Bedrohungsanalyse der letzten zehn Jahre immer weiter verfeinert. Dadurch hat sich diese Technologie zu einer Lösung für zielgerichtete Bedrohungen entwickelt, die ausgereift und fokussiert ist.

Das erkenntnisorientierte SOC für Unternehmen

Cyberkriminelle haben ihre Methoden angepasst, um herkömmliche Verteidigungssysteme zu umgehen, und legen sich unbemerkt monate- oder sogar jahrelang in Netzwerken auf die Lauer. Für die IT-Sicherheit in Unternehmen ist es an der Zeit, sich an diese Methoden wiederum anzupassen, indem sie einen erkenntnisorientierten, mehrstufigen Verteidigungsansatz verfolgen.

Bis vor Kurzem war es ausreichend, den Unternehmensperimeter durch den Einsatz allgemein verfügbarer Sicherheitstechnologien zu schützen, die Malware-Infektionen oder unbefugten Zugriff auf das Unternehmensnetzwerk verhindert haben. Heute jedoch ist dieser simple Ansatz durch das Aufkommen gezielter Angriffe nicht mehr ausreichend.

Wenn Ihre Sicherheitsabteilung Schutz vor neuen Gefahren bieten will, brauchen Sie einen vielseitigen, extrem anpassungsfähigen Sicherheitsansatz, der auf einem konventionellen SOC mit Threat Intelligence und mehrschichtigen Sicherheitslösungen basiert.

Verbesserung der Sicherheitsprozesse im Unternehmen

Die Abteilung für Datensicherheit ist für den organisatorischen und technischen Schutz kritischer Informationen und Geschäftsprozesse in oft komplexen IT-Umgebungen verantwortlich. Dazu gehören etwa der zunehmende Einsatz automatisierter Lösungen und Softwarekomponenten sowie der Übergang zum elektronischen Dokumentenmanagement.

Das explosionsartige Wachstum der Zahl fortgeschrittener Bedrohungen und zielgerichteter Angriffe hat auch zu einer steigenden Anzahl von Lösungen geführt. Um die generierten unstrukturierten Daten zu sammeln, zu speichern und zu verarbeiten und um komplexe Angriffe auf mehreren Ebenen zu erkennen und zu priorisieren, müssen bestehende Prozesse verbessert werden. Dazu zählen:

- die manuelle Priorisierung von Bedrohungen und die Bewertung von Faktoren, die auf einen potentiellen zielgerichteten Angriff hindeuten können
- das Sammeln von Informationen über gezielte Angriffe und hoch entwickelte statistische Bedrohungen;
- die Erkennung von Vorfällen und die Reaktion darauf;
- die Analyse verdächtiger Objekte im Netzwerkverkehr und in E-Mail-Anhängen
- die Erkennung von anormalen/ungewöhnlichen Aktivitäten innerhalb der geschützten Infrastruktur

Große Unternehmen reagieren auf aktuelle Bedrohungen, indem sie auf eine zentralisierte Informationssicherheits-Verwaltung umstellen, Daten aus getrennten Sicherheitslösungen konsolidieren (durch die Automatisierung der Datenerfassung und die Korrelation von Ereignissen, auch SIEM genannt) und die Präsentation dieser durch die Schaffung von Sicherheitsüberwachungszentralen (Security Operations Center, SOC) vereinheitlichen. Damit dieser Ansatz im Kampf gegen zielgerichtete Angriffe und hoch entwickelte Bedrohungen jedoch wirksam ist, ist ein umfassendes Verständnis von Sicherheitsproblemen und ein tiefgreifendes Wissen über die Analyse von Cyberbedrohungen erforderlich.

Kaspersky Lab war das erste technologieorientierte Unternehmen, das bereits 2008 ein dediziertes Labor für hoch entwickelte Bedrohungen eingerichtet hat.

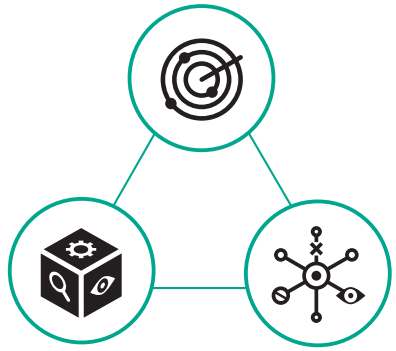
Dadurch haben wir mehr hoch entwickelte gezielte Bedrohungen entdeckt als andere Anbieter von Sicherheitslösungen.

Mit einer beeindruckenden Erfolgsbilanz bei der Erkennung von gezielten Angriffen und APTs ist unser GReAT-Team (Global Research and Analysis Team) für seine Threat Intelligence bekannt. Das Team war entscheidend an der Entdeckung vieler der raffiniertesten Angriffe beteiligt, darunter:

- Stuxnet
- RedOctober
- Flame
- Miniduke
- Epic Turla
- DarkHotel
- Duqu
- Carbanak
- Equation

... und viele mehr.

Kaspersky Anti Targeted Attack:
Schutz vor komplexen Bedrohungen



Kaspersky Cybersecurity Services: Security Insights oder Outsourcing

Kaspersky Endpoint Detection and Response: Vollständige Transparenz

Kaspersky Thread Management and Defense

Mit unserem genauen Verständnis der Funktionsweise vieler der weltweit raffiniertesten Bedrohungen haben wir, ein strategisch ausgerichtetes Portfolio aus Technologien und Services entwickelt, das ein vollständig integriertes, anpassungsfähiges Sicherheitsmodell möglich macht. Unsere Expertise ist der Grund dafür, dass Kaspersky Lab mehr erste Plätze bei unabhängigen Tests zur Erkennung und Abwehr von Bedrohungen erzielt hat als andere IT-Sicherheitsunternehmen. Nun haben wir unsere Expertise zur Erkennung gezielter Angriffe in einer eigenständigen Lösung zusammengefasst – das Ergebnis zweier Jahrzehnte der Bedrohungsforschung und -analyse zur Entwicklung ausgereifter, bewährter Technologien.

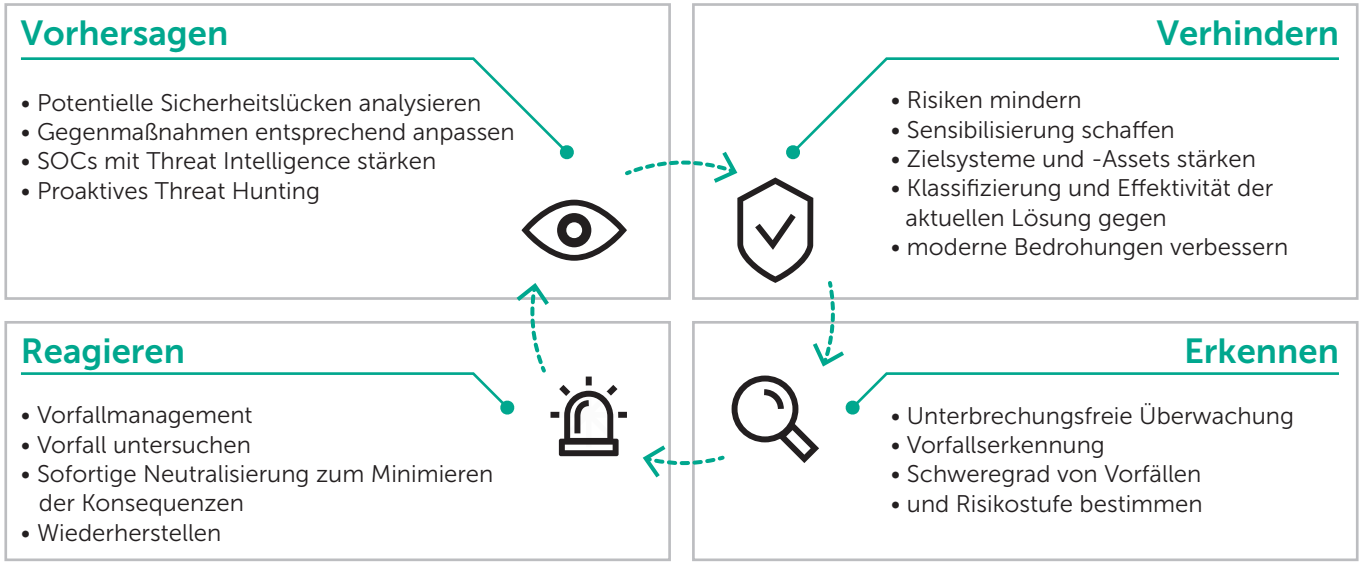
Während die überwiegende Mehrheit einfacher Cyberbedrohungen durch herkömmliche, signaturbasierte und durch heuristische Analysen ergänzte Sicherheitsprodukte blockiert werden kann, setzen die Cyberkriminellen und Hacker von heute immer raffiniertere Methoden ein, um bestimmte Organisationen zu treffen. Gezielte Angriffe, darunter hochentwickelte, hartnäckige Bedrohungen (Advanced Persistent Threats, APTs) – stellen eine der größten Gefahren für Unternehmen dar. Obwohl sich Bedrohungen – und die Techniken, die Cyberkriminelle und Hacker nutzen – ständig weiterentwickeln, versäumen es viele Unternehmen, ihre Sicherheitsstrategien an diese Entwicklung anzupassen.

Durch die Kombination von Erkennung auf mehreren Ebenen über die Kaspersky Anti Targeted Attack Platform und schneller Reaktion per Kaspersky Endpoint Detection and Response mit Cybersecurity Services und Premium Support bietet Kaspersky Threat Management and Defense eine einheitliche Lösung mit zentraler Verwaltung zur Automatisierung und Erleichterung des gesamten Verwaltungszyklus für hoch entwickelte Bedrohungen.

Gezielte Angriffe und hoch entwickelte Bedrohungen, die immer schwerer zu erkennen und häufig noch schwerer zu eliminieren sind, fordern eine umfassende, anpassungsfähige Sicherheitsstrategie. Kaspersky Threat Management and Defense basiert auf der von Gartner beschriebenen zukunftsweisenden Sicherheitsarchitektur. Unser Ansatz dabei ist, einen Maßnahmenzyklus in vier Schlüsselbereichen anzubieten: Verhindern, Erkennen, Reagieren und Vorhersagen.

- **Verhindern** – Reduzieren des Risikos hoch entwickelter Bedrohungen und gezielter Angriffe
- **Erkennen** – Identifizieren von Aktivitäten, die auf einen gezielten Angriff hinweisen könnten
- **Reagieren** – Schließen von Sicherheitslücken und Untersuchen von Angriffen
- **Vorhersagen** – Ermitteln, wo und wie neue zielgerichtete Angriffe auftreten könnten

Dies setzt im Wesentlichen voraus, dass traditionelle Präventionssysteme in Abstimmung mit Erkennungstechnologien, Bedrohungsanalysen, Reaktionsfunktionen und prädiktiven Sicherheitstechniken funktionieren. Auf diese Weise kann ein Cybersicherheitssystem geschaffen werden, das sich kontinuierlich an neue Herausforderungen für das Unternehmen anpasst und auf diese reagiert.



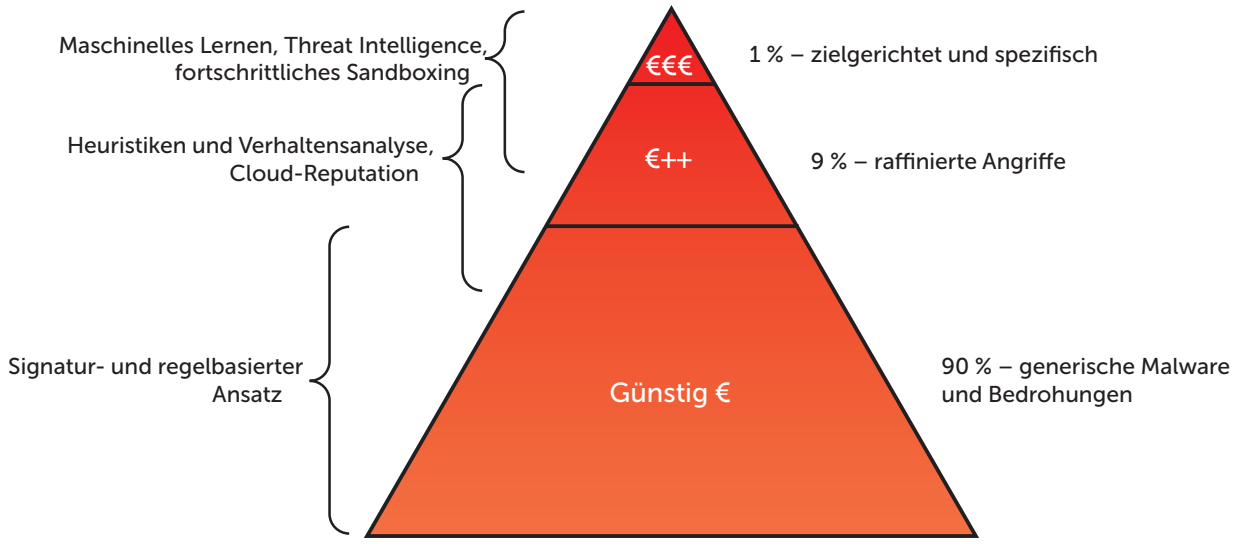
Prävention – Senken Sie das Risiko zielgerichteter Angriffe mit vielfach ausgezeichneten Sicherheitstechnologien

Bei zielgerichteten Angriffen sind Präventionstechnologien wertvoll, mit denen sich unnötige Vorfälle, gängige Schadobjekte und irrelevante Kommunikation filtern lassen.

Aber auch eine umfassende Systemhärtung mit gezielten Sicherheitslösungen, Sicherheitsschulungen und Sensibilisierung ist wertvoll. Sie erhöht den Zeit- und Investitionsaufwand, den Angreifer betreiben müssen, um Ihre kontrollierten Perimeter zu durchdringen, und macht Sie als Ziel für Angriffe unrentabel.

Präventionsbasierte Sicherheitsprodukte können sehr effektiv gegen gängige Bedrohungen wie Malware, Netzwerkangriffe, Datenlecks und vieles mehr schützen. Aber diese Technologien reichen nicht aus, um ein Unternehmen vor zielgerichteten Angriffen zu schützen. Bei einem zielgerichteten Angriff entdecken präventionsbasierte Sicherheitstechnologien möglicherweise einige Vorfälle, erkennen aber nicht, dass die einzelnen Vorfälle Teil eines weit gefährlicheren und komplexeren Angriffs sind, der dem Unternehmen beträchtlichen Schaden zufügen könnte.

Mehrstufige, präventionsbasierte Technologien sind jedoch nach wie vor ein Schlüsselelement des neuen, proaktiven Ansatzes zum Schutz vor zielgerichteten Angriffen.



Mit Sicherheitstechnologien gegen verschiedene Bedrohungen vorgehen

80 % der zielgerichteten Angriffe beginnen mit einer schädlichen E-Mail, die einen Anhang oder Link enthält.

Bevorzugte Penetrationsziele für Cyberkriminelle sind Personalabteilungen, Callcenter, persönliche Assistenten der Geschäftsleitung und ausgelagerte Bereiche des Unternehmens. Diese gelten als die am schlechtesten vorbereiteten Bereiche einer Organisation.

Für Unternehmen ist es unerlässlich, weiterhin „traditionelle" Sicherheitstechnologien einzusetzen, um:

1. das Filtern und Blockieren von Ereignissen und Vorfällen, die nicht mit zielgerichteten Angriffen zusammenhängen, zu automatisieren. Auf diese Weise werden unnötige Ablenkungen bei der Aufdeckung relevanter Vorfälle vermieden.

2. die IT-Infrastruktur gegen billige und leicht durchführbare Techniken abzuhärten (Social Engineering, Wechseldatenträger, mobile Geräte, Malware, Zustellung schädlicher E-Mails usw.). Alle bisherigen Ausgaben für die Perimeter- und Endpoint-Sicherheit sowie die eingerichteten Kontrollsysteme tragen in der Tat dazu bei, den Aufwand und die Investitionen zu erhöhen, die Cyberkriminelle benötigen, um in Ihr Netzwerk einzudringen.

Wenn der Angreifer jedoch ausreichend motiviert ist und vielleicht sogar von einem Dritten angeheuert wird, um einen erfolgreichen Angriff durchzuführen, wird ein reiner Präventionsansatz nicht ausreichen.

Erkennung – Hoch entwickelte Multi-Vektor-Bedrohungen erkennen, bevor ein Schaden verursacht wird

Die Kaspersky Anti Targeted Attack Platform umfasst:

- **Mehrstufige Sensorarchitektur** für umfassende Transparenz. Durch die Kombination von Netzwerk-, Web-, E-Mail- und Endpoint-Sensoren bietet KATA hoch entwickelte Erkennung auf allen Ebenen Ihrer IT-Infrastruktur.
- **Advanced Sandbox** – zur Beurteilung neuer Bedrohungen. Unsere Advanced Sandbox ist das Ergebnis einer mehr als zehn Jahre langen, kontinuierlichen Entwicklung und bietet eine isolierte, virtualisierte Umgebung, in der verdächtige Objekte sicher verwahrt und so ihre Verhaltensweise beobachtet werden kann.
- **Leistungsstarke analytische Engines** für schnelle Ergebnisse und weniger Fehlalarme.
  Unser Targeted Attack Analyzer bewertet Daten von Netzwerk- und Endpoint-Sensoren und erstellt rasch die Ergebnisse der Bedrohungserkennung für das Sicherheitsteam.

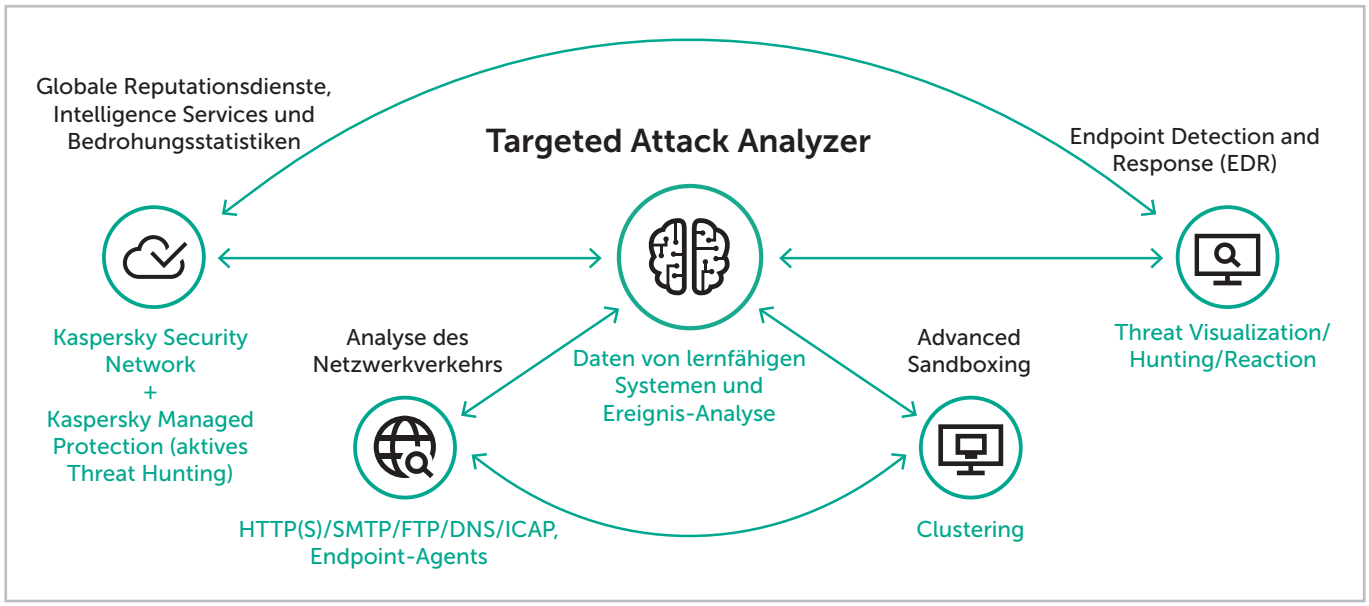
Je früher ein Angriff erkannt wird, desto geringer sind Ihre finanziellen Verluste und desto weniger Störungen treten in Ihrer Organisation auf. Deshalb ist die Qualität und Effektivität der Erkennung von höchster Wichtigkeit.

Da gezielte Angriffe äußerst komplex sind, erfordert ihre Erkennung ein tiefgreifendes Praxiswissen über die Funktionsweise hoch entwickelter und gezielter Angriffe. Einfache Anti-Malware-Lösungen können keinen Schutz vor diesen Angriffsarten bieten. Stattdessen benötigen Sie Erkennungstechnologien, die auf minütlich aktuelle Bedrohungsinformationen zugreifen und detaillierte Analysen eines verdächtigen Verhaltens ausführen können, das auf verschiedenen Ebenen des Unternehmensnetzwerks auftreten kann.

Um zielgerichtete Angriffe erkennen zu können, sind miteinander verbundene Lösungen und Services erforderlich, die Folgendes bieten können:

- **Schulungen**
- **Fachwissen über Targeted Attack Discovery**: einmalige Überprüfung der Infrastruktur, um Spuren von Sicherheitsverletzungen zu finden
- **Spezialisierte Lösung**: Kaspersky Anti Targeted Attack Platform + Kaspersky Endpoint Detection and Response
- **Threat Data Feeds** für den Echtzeit-Austausch von Bedrohungsinformationen und Updates über neue Bedrohungen
- **Benutzerdefinierte und APT-Berichte** zum besseren Verständnis von Bedrohungsquellen und -methoden
- **Threat Hunting rund um die Uhr**: Kaspersky Managed Protection Service

Die Kaspersky Anti Targeted Attack Platform basiert auf führender Security Intelligence sowie fortschrittlichen lernfähigen Technologien und kombiniert Netzwerk- und Endpoint-Daten, Sandboxing und intelligente Analyse, um Vorfälle zu korrelieren, nach Gefährdungsindikatoren zu suchen und auch komplexeste gezielte Angriffe aufzudecken. Die Verknüpfung der verschiedenen Teile eines Vorfalls bietet einen umfassenden Überblick über die gesamte Angriffskette, erhöht das Vertrauen in zugeteilte Bedrohungsbewertungen und reduziert Fehlalarme auf null.

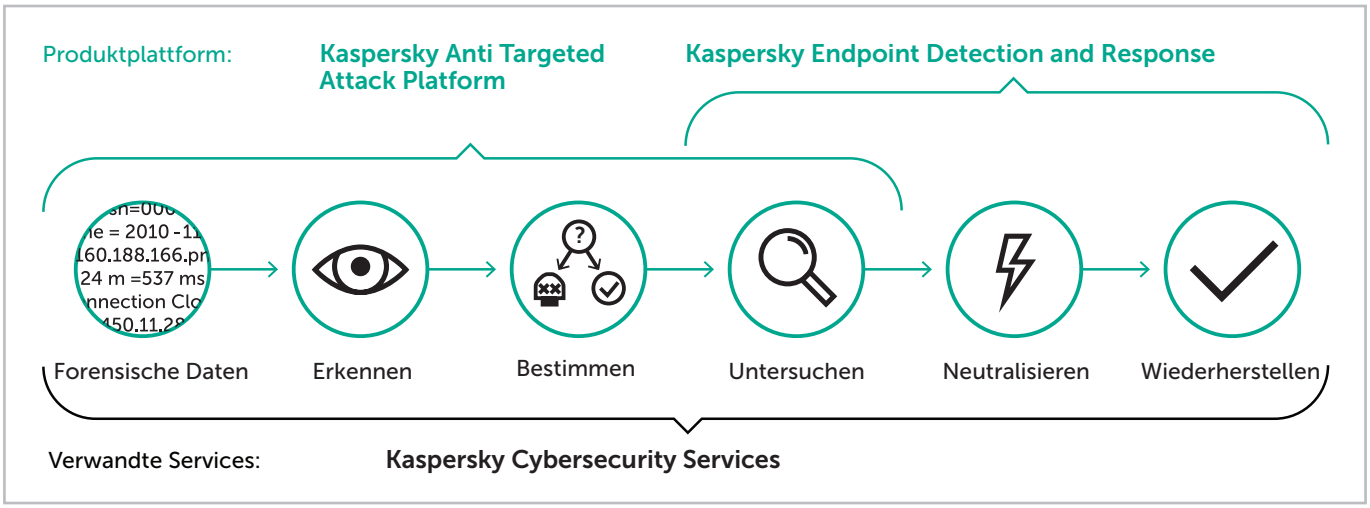


Reaktion – Unterstützung von Unternehmen bei der Beseitigung der Folgen von Angriffen

Höhere Erkennungsraten sind wichtig, aber nur ein Teil der erforderlichen Abwehrmaßnahmen. Die besten Erkennungstechnologien nützen nicht viel, wenn Sie nicht die erforderlichen Tools und Kenntnisse haben, um rasch auf die „Live"-Bedrohung zu reagieren, die eine potentielle Gefahr für Ihre Organisation darstellt.

Nachdem Sie einen Angriff erkannt haben, brauchen Sie Sicherheitsexperten, die die Fähigkeiten und die Erfahrung besitzen, Sie bei Folgendem zu unterstützen:

- Prüfung und Beseitigung des Schadens
- Schnelle Wiederaufnahme Ihrer Betriebsabläufe
- Bereitstellung praktisch umsetzbarer Informationen nach der Vorfallsuntersuchung
- Planung von Maßnahmen, um eine Wiederholung desselben Angriffs zu verhindern

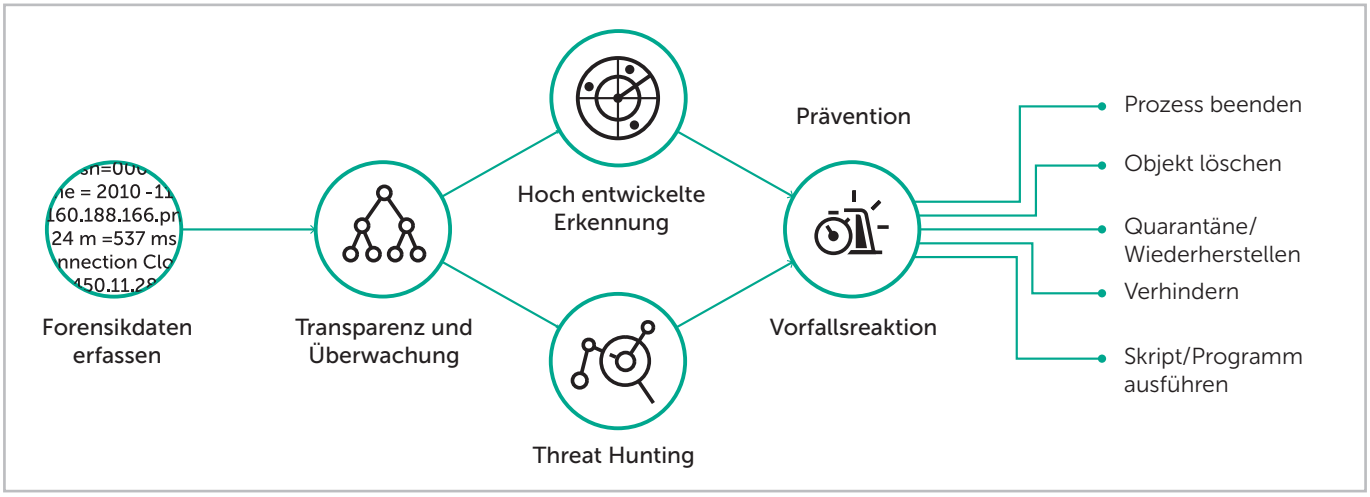


Kaspersky Endpoint Detection and Response bietet:

- **Hoch entwickelte Erkennung** mit lernfähigen Systemen – Targeted Attack Analyzer (TAA) – erstellt eine Baseline für Endpoint-Verhalten. Dies ermöglicht es, einen Verlauf zu erstellen, anhand dessen festgestellt werden kann, wie ein Verstoß erfolgte.
- **Proaktives Threat Hunting** mit schneller Suche unter Verwendung einer zentralen Datenbank sowie Gefährdungsindikatoren-Suche (IoC), die das Sicherheitsteam bei der aktiven Suche nach Bedrohungen unterstützt, für proaktives Scannen von Endpoints, um Anomalien und Sicherheitsverletzungen aufzuspüren
- **Adaptive Threat Response** umfasst eine große Anzahl automatisierter Reaktionen, dank derer Unternehmen herkömmliche Beseitigungsmechanismen – wie z. B. Löschung und Re-Imaging – und damit einhergehende kostspielige Ausfallzeiten und Produktivitätsverluste vermeiden können.

Sobald die Kaspersky Anti Targeted Attack Platform oder die Sicherheitslösung eines Drittanbieters feststellt, dass Ihr Unternehmen angegriffen wird, übernimmt Kaspersky Endpoint Detection and Response. Es ist die nächste essentielle Komponente von Threat Management and Defense, mit der Unternehmen ihre Vorfallsreaktion beschleunigen und die Qualität der Untersuchung von Cybersicherheitsvorfällen verbessern können.

Kaspersky EDR bietet zentralisiertes Incident Management für alle Endpoints des Unternehmensnetzwerks – für einen nahtlosen Workflow und die Integration mit der Netzwerkerkennung über die Kaspersky Anti Targeted Attack Platform. Durch eine Vielzahl an automatisierten Reaktionen können teure Ausfallzeiten und Produktivitätsverluste, die mit traditionellen Beseitigungsmechanismen wie etwa dem Löschen und Re-Imaging verbunden sind, verhindert werden. Durch die Überwachung und Kontrolle einer Vielzahl an Funktionen über eine zentrale Oberfläche können Sie Sicherheitstasks effektiver und effizienter durchführen – ohne zwischen mehreren Tools und Konsolen wechseln zu müssen.



Vollständige Transparenz und präzise Erkennung sind nur ein Teilaspekt des Kampfes. Die Angreifer, die hinter zielgerichteten Angriffen stehen, kehren naturgemäß mit neuen Werkzeugen und Techniken zurück. Im Ernstfall benötigt das Cybersicherheits-Team möglicherweise einen vertrauenswürdigen Partner mit den entsprechenden Fähigkeiten und Erfahrungen und muss außerdem interne Fähigkeiten weiterentwickeln.

Unser Incident Response Service umfasst Folgendes:

- **Vorfallsprüfung:** Anfängliche Analyse eines Vorfalls, die schnell bereitgestellt wird, um Sie dabei zu unterstützen, den Schaden für Ihr Unternehmen zu minimieren (die Analyse kann vor Ort oder per Fernzugriff durchgeführt werden).

- **Beweissammlung:** Dies schließt das Sammeln von Images der Festplattenlaufwerke sowie von Speicherabbildern, Netzwerk-Traces und anderen Informationen ein, die für den Vorfall relevant sind.

- **Forensische Analyse:** Detaillierte Analyse zur Erfassung der folgenden Informationen:
  - Was wurde angegriffen?
  - Wer hat den Angriff ausgeführt?
  - Über welchen Zeitraum wurde Ihr Unternehmen angegriffen?
  - Wo liegt der Ursprung des Angriffs?
  - Warum wurde Ihr Unternehmen angegriffen?
  - Wie wurde der Angriff implementiert?

- **Malware-Analyse:** Detaillierte Analyse der Malware, die als Bestandteil des Angriffs eingesetzt wurde.

- **Schadensregulierungsplan:** Ein detaillierter Plan, der Ihr Unternehmen dabei unterstützt, die Verbreitung von Malware in Ihrem Netzwerk zu verhindern und einen Deinstallationsplan zu erstellen.

- **Untersuchungsbericht:** Ein detaillierter Bericht, der Informationen zur Vorfallsuntersuchung und zu Korrekturmaßnahmen enthält.

Wenn Ihr eigenes Sicherheitsteam in der Lage ist, viele der Aufgabe der Vorfallsreaktion durchzuführen, möchten Sie möglicherweise einen unserer anderen Dienste verwenden:

- **Malware-Analyse-Service**: führt detaillierte Analysen der Malware aus, die Ihr Team isoliert hat.

- **Digitaler Forensik-Service**: analysiert digitale Nachweise und Vorfallseffekte, die von Ihrem Team gesammelt wurden.

Prävention – besserer Schutz vor künftigen Bedrohungen

Mit der sich ständig ändernden Bedrohungslandschaft muss auch Ihre Sicherheitsstrategie ständig weiterentwickelt und an die neuen Herausforderungen angepasst werden.

Die Etablierung von Sicherheitsmaßnahmen ist keine einmalige Aktivität, sondern ein fortlaufender Prozess, der ein ständiges Assessment der folgenden Elemente erfordert:

- Aktuelle Bedrohungen
- Effektivität der IT-Sicherheit

Nur so kann Ihr Unternehmen auf neue Risiken und die sich ändernden Anforderungen abgestimmt werden.

Zugriff auf globale Threat Intelligence mit Kaspersky Lab

Die Zusammenarbeit mit Experten, die Sie in Bezug auf die globale Bedrohungslandschaft auf dem aktuellen Stand halten können und Sie beim Testen Ihrer Systeme und Ihrer bestehenden Abwehr unterstützen, ist unerlässlich, damit Ihre Organisation mit den sich ständig weiterentwickelnden Bedrohungen Schritt halten und sich auf diese einstellen kann.

Im Laufe der Jahre haben unsere Sicherheitsexperten weltweit ein umfangreiches Wissen über die Funktionsweise von hoch entwickelten und gezielten Angriffen erworben. Außerdem analysieren wir ständig neue Angriffstechniken. Durch diese hart erarbeitete Expertise sind wir bestens aufgestellt, um neue Angriffsmethoden vorherzusagen und Sie bei ihrer Abwehr zu unterstützen.

Darüber hinaus bieten wir die folgenden Cybersecurity Services zur Stärkung Ihrer IT-Infrastruktur:

- Penetrationstests, um Sie bei der Bewertung der Effektivität Ihrer aktuellen Sicherheitsmaßnahmen zu unterstützen
- Application Security Assessment, um Sie bei der Identifizierung von Softwareschwachstellen zu unterstützen, bevor diese von Cyberkriminellen entdeckt werden
- fortgeschrittenes Cybersecurity Training, um Sie beim Schulen Ihrer eigenen Experten und beim Aufbau eines eigenen Security Operations Center zu unterstützen
- Threat Data Feeds und kundenspezifische Bedrohungsberichte, um Sie in Bezug auf die sich ständig ändernde Bedrohungslandschaft stets auf dem aktuellen Stand zu halten
- Threat-Lookup-Portal mit Zugriff auf die globale Threat-Intelligence-Datenbank von Kaspersky Lab, um Ihre Malware-Forschung zu unterstützen

Die anpassungsfähige Sicherheitsstrategie von Kaspersky Lab basiert auf der von Gartner beschriebenen zukunftsweisenden Sicherheitsarchitektur. Der Ansatz von Kaspersky Lab ist dabei, einen Maßnahmenzyklus in vier Schlüsselbereichen anzubieten: Verhinder, Erkennen, Reagieren und Vorhersagen. Dies setzt im Wesentlichen voraus, dass traditionelle Präventionssysteme in Verbindung mit Erkennungstechnologien, Bedrohungsanalysen, Reaktionsfunktionen und vorausschauenden Sicherheitstechniken funktionieren. Auf diese Weise kann ein Cybersicherheitssystem geschaffen werden, das sich kontinuierlich an die neuen Herausforderungen für das Unternehmen anpasst und auf diese reagiert.

Der Einsatz von Threat Management und Defense von Kaspersky Lab bringt folgende Vorteile mit sich:

1. Übergang von einem reaktiven Sicherheitsmodell zu einem proaktiven Modell auf der Grundlage von Risikomanagement, unterbrechungsfreier Überwachung, fundierter Vorfallsreaktion und Threat-Hunting-Funktionen.

2. Ihr operatives Framework optimiert die täglichen Sicherheitsprozesse und erhöht die Sicherheit durch ein mehrstufiges Verteidigungsmodell, das hoch entwickelte Bedrohungen in jedem Stadium des Angriffs verhindert und erkennt.

3. Eine integrierte Plattform reduziert die vielen Sicherheitswarnungen, die die meisten Sicherheitsteams überfordern, durch Threat-Intelligence-basierten Kontext und die Priorisierung von Warnungen. Taktische Reaktionen werden durch den Informationsaustausch über Bedrohungen, fundiertes Fachwissen und die Bereitstellung von Security Intelligence Services verbessert.

4. Diese Umgebung bietet Sicherheitsanalysten zentralen Einblick in alle Phasen eines Angriffs und ermöglicht eine nahtlose Bedrohungsanalyse sowie die zuverlässige Untersuchung sowohl bekannter als auch unbekannter Bedrohungen, bevor sich diese auf das Unternehmen auswirken.

5. Die Weitergabe von Global Threat Intelligence über APT und Threat-Intelligence-Portale liefert einzigartige, proaktive Einblicke in die Motive und Absichten Ihrer Gegner, sodass Sie Richtlinien und die Planung von Sicherheitsinvestitionen entsprechend priorisieren können.

Globale Kompetenz mit Technologien von Kaspersky Lab

Die Wirksamkeit der Produkte von Kaspersky Lab wird regelmäßig durch die Ergebnisse unabhängiger Tests bestätigt. Im Jahr 2015 rangierte das Unternehmen unter den drei bestbewerteten Anbietern von Sicherheitslösungen ganz oben. Den Ergebnissen von 84 verschiedenen Tests nach, die von angesehenen Testorganisationen in mehreren Ländern durchgeführt wurden, erreichten die Lösungen von Kaspersky Lab in 82 % der Tests einen Platz unter den top drei und belegten 60 Mal den ersten Platz. Das ist ein unwiderlegbarer Beweis dafür, dass Kaspersky Lab den besten Schutz der Branche bietet.

Bewährte Lösungen gegen hoch entwickelte Bedrohungen

Im Laufe des Jahres 2017 wurde unsere Kaspersky Anti-Targeted Attack Platform (als Teil von Threat Management and Defense) weiterhin Tests durch ICSA Labs unterzogen.

Die letzten Tests dauerten 37 Tage und bestanden aus 585 Angriffen und 519 sauberen Dateien. KATA lieferte hervorragende Ergebnisse:

- perfekte Erkennungsrate von 100 % (NULL übersehene Proben)
- minimale Fehlalarmrate von 0 %
- Status „Zertifiziert" erreicht

Im Folgenden ein paar Auszüge aus dem ICSA-Bericht vom 7. Juli:

- „Die Lösung von Kaspersky hat sich in diesem Testzyklus hervorragend bewährt"
- „Die KATA-Plattform von Kaspersky Lab erkannte 100,0 % der Bedrohungen, die während des Tests auftraten – ein wesentlich höherer Prozentsatz, als für die Zertifizierung erforderlich war."
- „KATA von Kaspersky Lab zeigte hervorragende Wirksamkeit bei der Erkennung von fast 600 neuen und wenig bekannten Bedrohungen."
- „Egal, wie neu oder alt die Bedrohung war, die KATA-Plattform von Kaspersky Lab erkannte alle neuen und wenig bekannten schädlichen Bedrohungen."
- „Die Kaspersky KATA-Plattform löste in diesem Testzyklus keinerlei Fehlalarme aus – ein hervorragendes Ergebnis."
- „KATA Advanced Threat Defense von Kaspersky Lab hat alle Testfälle bestanden, die für eine ICSA Labs Advanced Threat Defense-Rezertifizierung erforderlich sind. Der erfolgreiche Abschluss dieses Testzyklus kennzeichnet das dritte Quartal in Folge, in dem Kaspersky Lab die ATD-Zertifizierungskriterien von ICSA Labs erfüllt hat."

HINWEIS: Das ICSA-Testverfahren ist dynamisch und ändert sich von Quartal zu Quartal. Der Test selbst ist eine sich ständig weiterentwickelnde Simulation einer realen Umgebung und diverser Angriffsmethoden. Die Sicherheit wird nicht zu einem bestimmten Zeitpunkt, sondern über einen langen Zeitraum (mehr als 30 Tage) im Dauerbetrieb und mit zahlreichen Angriffen gemessen. Auf diese Weise soll der Test die Effizienz und Wirksamkeit einer Lösung aus Anwendersicht demonstrieren.

Visionärer und umfassender Ansatz

Seit mehreren Jahren führt die Radicati Group eine unabhängige Analyse des Marktes für APT-Schutzlösungen durch, die Branchenführer (Top Players), Pioniere (Trail Blazers), Spezialisten (Specialists) und erfahrene Anbieter (Mature Players) ermittelt. Im Ergebnis der soeben veröffentlichten Marktanalyse wurde der Ansatz von Kaspersky Lab zur Abwehr von zielgerichteten Angriffen und hoch entwickelten Bedrohungen hervorragend bewertet.

Im Jahr 2017 verbesserte Kaspersky Lab seine Position deutlich mit einem großen Schritt vom Spezialisten hin zum führenden Pionierunternehmen auf dem Gebiet.

Pionierunternehmen bieten in einigen Bereichen ihrer Lösungen die fortschrittliche und führende Technologien an, verfügen aber nicht unbedingt über all die Funktionen, die nötig sind, um sich als Branchenführer zu positionieren. Pionierunternehmen haben jedoch das Potential, den Markt mit neuen Technologien oder neuen Bereitstellungsmodellen in Aufruhr zu versetzen. Im Laufe der Zeit werden diese Anbieter sehr wahrscheinlich zu Branchenführern.

„Die Kaspersky Anti Targeted Attack Platform bietet eine fortschrittliche Erkennung hoch entwickelter Bedrohungen und zielgerichteter Angriffe auf allen Ebenen eines gezielten Angriffs – von der Erstinfektion über die Befehls- und Steuerungskommunikation bis hin zu horizontaler Infiltrierung und Datenausschleusung."

Kaspersky Lab
Cybersicherheit für Unternehmen:
www.kaspersky.de/enterprise
Neues über Cyberbedrohungen: **de.securelist.com**
IT-Sicherheitsnachrichten:
https://www.kaspersky.de/blog/b2b/

#truecybersecurity
#HuMachine

www.kaspersky.de