Bedrohungen proaktiv aufspüren

Umfassender Schutz vor bekannten und fortgeschrittenen Bedrohungen als Managed Service rund um die Uhr

Kaspersky MDR: die Highlights

- Schnelle, skalierbare IT-Sicherheitsfunktionen
- Keine zusätzlichen Investitionen oder Mitarbeitende notwendig
- Erstklassiger Schutz vor sehr komplexen und innovativen Bedrohungen
- Verhindert Unterbrechungen des Geschäftsbetriebs
- Vollständig gemanagter oder angeleiteter Umgang mit Sicherheitsvorfällen
- Transparenz über die aktuelle Situation aller Assets und deren Schutzstatus
- Arbeitet mit Kaspersky Endpoint Security, EDR und Anti Targeted Attack zusammen

Kaspersky wurde 1997 in Moskau gegründet. Heute agiert der Sicherheitsspezialist in 200 Ländern, beschäftigt über 4000 hoch qualifizierte Spezialisten und Spezialistinnen und gilt als führender Anbieter von Sicherheitslösungen für Privatanwender, KMU und Grossbetriebe. Kaspersky-Technologien schützen weltweit um die 400 Millionen User und stehen in mehr als 270 000 Unternehmen und Organisationen im Einsatz. Die Cybersecurity-Lösungen und Cybersecurity-Dienste von Kaspersky umfassen cloudbasierte, als Managed Service sowie On-Premises betriebene Endpoint Security, Hybrid Cloud Security und Enterprise Security der nächsten Generation inklusive Lösungen zur Absicherung von IoT- und industriellen Anwendungen. Im Hintergrund stehen dabei stets die langjährige Expertise der Kaspersky-Professionals und die tief greifende Threat Intelligence, die aus den global gewonnenen Cybersicherheitsdaten der eingesetzten Lösungen resultiert. Kaspersky Managed Detection and Response (MDR) entlastet die Sicherheitsverantwortlichen massgeblich und stellt skalierbare Security-Funktionalität als Managed Service in der Cloud bereit. MDR schützt vor komplexen und unerkannten Bedrohungen und verhindert, dass diese im Unternehmensnetz Schaden anrichten und den Geschäftsbetrieb beeinträchtigen können – und dies ohne Investitionen in zusätzliche Infrastruktur oder Mitarbeitende. Darüber hinaus verschafft die Lösung über anschauliche Dashboards umfassende Transparenz über den aktuellen Sicherheitsstatus aller Assets und erlaubt, auf Sicherheitsvorfälle automatisiert oder angeleitet zu reagieren.

Bequeme Sicherheit mit Managed Detection and Response

Die meisten Sicherheitsteams reagieren erst auf Cybersicherheitsvorfälle, nachdem sie bereits eingetreten sind. In der Zwischenzeit bleiben neue Bedrohungen unter dem Radar und vermitteln ein falsches Gefühl von Sicherheit. Mit Kaspersky Managed Detection and Response lassen sich Bedrohungen, die unerkannt, aber noch immer aktiv in der IT-Infrastruktur lauern, proaktiv aufspüren.

So funktioniert Kaspersky MDR

Managed Detection and Response arbeitet mit den Endpoint-Security-Lösungen von Kaspersky zusammen und überprüft die von den Produkten ausgegebenen Warnmeldungen. Dabei werden auch die Metadaten von Systemaktivitäten auf Anzeichen aktiver oder bevorstehender Angriffe untersucht.

Die Metadaten werden über das Kaspersky Security Network erfasst und in Echtzeit automatisch mit der stets aktuellen Threat Intelligence abgeglichen, um Taktiken, Techniken und Vorgehensweise von Angreifern zu erkennen. Von Kaspersky selbst entwickelte Angriffsindikatoren sorgen dafür, dass im Verborgenen lauernde Bedrohungen abseits von Malware, die legitime Aktivitäten vortäuschen, erkannt werden. Innerhalb der ersten zwei bis vier Wochen passt sich das Produkt an die Infrastruktur an, um eine False-positive-Rate von Null zu erreichen. Dabei stimmt es mit dem Sicherheitsteam ab, was legitim ist und was nicht.

Zwei Varianten: Optimum und Expert

Kaspersky MDR ist in zwei abgestuften Varianten für unterschiedliche Ansprüche und Unternehmensgrössen verfügbar.

Kaspersky MDR Optimum erhöht unmittelbar den Sicherheitsstatus der IT-Systeme, ohne dass in zusätzliche Mitarbeitende oder externe Expertise investiert werden muss.

Kaspersky MDR Expert bietet darüber hinaus weitere Funktionen sowie Flexibilität für erfahrene IT-Sicherheitsteams, die die Auswahl und Untersuchung von Vorfällen an Kaspersky abgeben und ihre begrenzten eigenen IT-Sicherheitsressourcen so auf die Abwehr der ihnen vorgelegten kritischen Fälle richten können.

Zur weiteren Überprüfung, Untersuchung und Identifizierung neuer Bedrohungen nutzt die Threat-Hunting-Funktion bei MDR Optimum eine automatisierte Erkennungsfunktion, die mit eigens ermittelten Angriffsindikatoren arbeitet. In MDR Expert basiert die Managed-Threat-Hunting-Funktion auf der aufwendigen Handarbeit der erfahrenen Experten und Expertinnen von Kaspersky, die proaktiv solche Bedrohungen aufspüren, welche die automatische Erkennung umgehen.

Dazu kommen optionale Komponenten. So unter anderem eine Option zur gesetzeskonformen Speicherung der Daten, ein Incident Response Retainer, ein umfassendes Gefährdungsassessment sowie Schulungen für SOC-Analysten.