ESG SHOWCASE

Warum MDR ein wichtiger Bestandteil moderner Cybersicherheitsstrategien ist

Datum: August2022 **Autor:** Dave Gruber, ESG Principal Analyst

KURZFASSUNG: Die Bedeutung von Erkennungs- und Reaktionsfunktionen in einem Cybersicherheitsprogramm ist absolut unstrittig. Die große Herausforderung besteht darin, wie sich eine zeitnahe, präzise, zuverlässige und konsistente Erkennung und Reaktion am besten sicherstellen lässt, wenn sich die Anzahl der Bedrohungen multipliziert und deren Komplexität schneller zunimmt, als die meisten Unternehmen sich anpassen können. Managed Detection and Response (MDR) als Managed Service über Drittanbieter bietet einen Ansatz, damit die Unternehmen Schritt halten können.

Einführung: Der Aufstieg von MDR

Alle Unternehmen sind mit einer klaren Realität konfrontiert: Cybersicherheitsbedrohungen nehmen rasant zu und auch die Angriffsflächen werden größer. Herkömmliche Prozesse und Tools zur Erkennung von und Reaktion auf Bedrohungen reichen heute nicht mehr aus. Sowohl die Bedrohungen selbst als auch die dahinterstehenden böswilligen AkteurInnen werden immer versierter, agiler und persistenter. Sie schaffen ein digitales bewegliches Ziel für Sicherheits- und IT-ExpertInnen, die für den Schutz der Unternehmensressourcen zuständig sind.

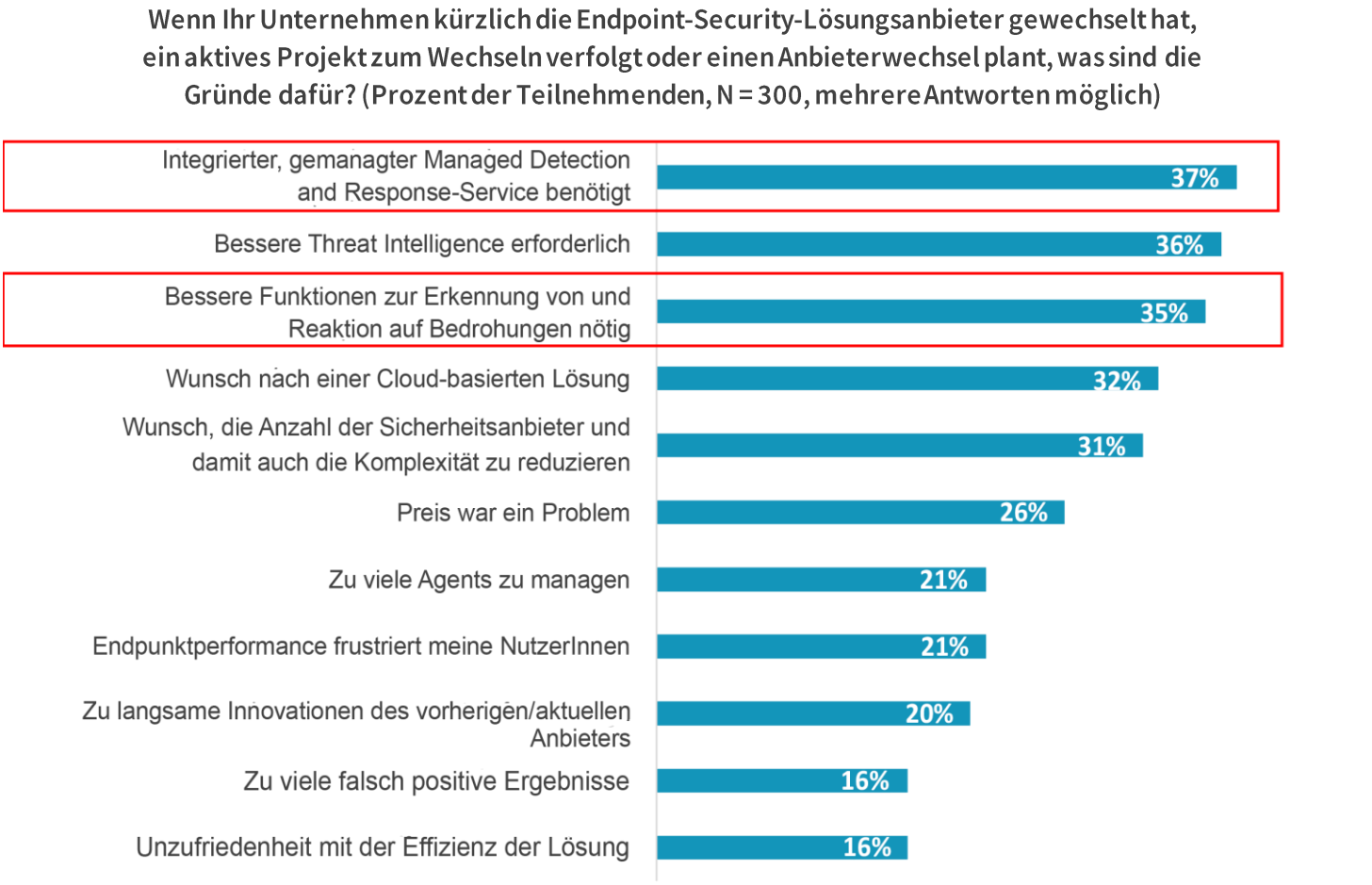
Eine Vielzahl von Sicherheitskontrollen erhöht die Kosten und die Komplexität der Erkennungs- und Reaktionsbemühungen, da die Sicherheitsteams eine konstante Flut an Warnmeldungen manuell auswerten müssen, um tatsächliche Bedrohungen von falsch positiven Ergebnissen zu unterscheiden. Der Aufbau eines größeren SOC (Security Operations Center) und der Einsatz von weiteren Tools und mehr SicherheitstechnikerInnen ist teuer – vorausgesetzt, dass Unternehmen angesichts des enormen und weiter zunehmenden Fachkräftemangels im Bereich der Cybersicherheit überhaupt genügend SicherheitsexpertInnen finden und einstellen können.

Aufgrund der Neugestaltung ihrer Cybersicherheitsprogramme wenden sich Unternehmen immer häufiger an Anbieter von Managed Detection and Response-Lösungen, um Hilfe zu erhalten.

Aufgrund der Neugestaltung ihrer Cybersicherheitsprogramme wenden sich Unternehmen immer häufiger an Anbieter von Managed Detection and Response-Lösungen, um Prozesse zu verfeinern, Ressourcen- und Kompetenzlücken zu schließen und Sicherheitstools zu modernisieren. Viele verbinden MDR mit Endpoint Security, da die ESG-Studie aufgezeigt hat, dass die Notwendigkeit eines integrierten MDR-Service ein wichtiger Faktor ist, aus dem Unternehmen ihre Endpoint-Security-Lösungsanbieter wechseln (siehe Abbildung 1).[1]

[1] Quelle: ESG Complete Survey Results, *Endpoint Security Trends*, Dezember2021. Alle ESG-Studienreferenzen und -Diagramme in diesem Showcase stammen aus diesen Umfrageergebnissen.

Abbildung 1: Hauptgründe für den Wechsel der Endpoint-Security-Anbieter



Quelle: ESG, eine Division von TechTarget, Inc.

Da Sicherheitsteams die Erkennungs- und Reaktionsprogramme erweitern und auf umfassendere XDR(Extended Detection and Response)-Lösungen upgraden, bieten MDR-Angebote Unternehmen die Möglichkeit, sowohl die Technologie als auch ihre Betriebsmodelle zu aktualisieren, um so die Angriffsfläche umfassender zu schützen und die Bedrohungserkennung zu verbessern. Neue Ansätze sind erforderlich, die Rund-um-die-Uhr-Monitoring, globale Threat Intelligence in Echtzeit, Automatisierung und moderne ML-Analysen kombinieren – natürlich zusammen mit der Fähigkeit, enorme Mengen an Sicherheitstelemetriedaten zur Unterstützung einer schnellen Bedrohungserkennung und -suche verarbeiten zu können. Während sich XDR weiterentwickelt und ausgefeilter wird, können Unternehmen jeder Größe und mit jeder Sicherheitsstufe mithilfe der MDR-Services die Erkennung und Reaktion operationalisieren und das Risiko von Advanced Threats mindern. Das ist besonders wichtig, weil die Unternehmen die Grenzen der Cybersicherheit in Bezug auf Umfang und Skalierung vom Rechenzentrum über den Edge bis zur Cloud neu definieren. MDR führt die MitarbeiterInnen, Prozesse und Technologien zusammen, die benötigt werden, um Anwendungsfälle für die Erkennung von und Reaktion auf Bedrohungen auf verteilte Unternehmen auszuweiten.

Wichtige Faktoren für die MDR-Einführung

Die Nutzung von MDR-Services nimmt zu und bietet Sicherheitsteams einen Weg, die Abdeckung zu erweitern, Personallücken zu schließen und die übergeordneten Programmziele zu stärken. Die Anwendungsfälle variieren zwar, aber das sind die zugrunde liegenden Treiber:

- **Bedrohungslandschaft:** Die Anzahl der Cyberangriffe und deren zunehmende Ausgefeiltheit haben Unternehmen unter enormen Druck gesetzt, sie schneller und definitiver zu erkennen und darauf zu reagieren.
- **Feindliche Absicht:** Die AngreiferInnen sind in Bezug auf die Planung und Durchführung ihrer Angriffe intelligenter, persistenter und noch strategischer geworden. Sie haben ein leistungsstarkes „kriminelles Netzwerk" geschaffen, in dem böswillige AkteurInnen Taktiken austauschen und sogar bei Angriffen zusammenarbeiten.
- **Wirtschaft:** Die CAPEX-Verpflichtung zum Aufbau und zur Erweiterung eines SOC ist beträchtlich – in der Regel geht es um siebenstellige Ausgaben, teilweise noch höher.
- **Aktualisierung der Cybersicherheitstechnologie:** Unternehmen, die alle oder den Großteil der Sicherheitsabläufe intern durchführen, müssen die Kontrollmechanismen für Cybersicherheit häufiger aktualisieren. Das umfasst auch die Umstellung der Endpunkterkennung und -reaktion der ersten Generation zu einem umfassenderen XDR-/MDR-Framework.
- **Fachkräftemangel:** Der viel diskutierte Fachkräftemangel im Bereich der Cybersicherheit ist ein andauerndes Problem. Wenn interne Cybersicherheitspositionen nicht ordnungsgemäß besetzt werden können, führt das häufig zu Herausforderungen bei erkennungs- und reaktionsbezogenen Zielen, was wiederum die Ressourcen gefährdet.

Cyberangriffe erfolgen wahllos. Kleine und mittelständische Unternehmen mit begrenztem Personal und Budget sowie früher erfolgten Angriffen sind gefährdet. Selbst sehr große Unternehmen benötigen zusätzliches Personal, skalierbare Kontrollen und strategische Beratungen auf Führungsebene, um die sich entwickelnde Bedrohungslandschaft zu erkennen und darauf zu reagieren.

Worauf Sie bei einem MDR-Service und einem MDR-Serviceanbieter achten sollten

Es gibt einige wichtige und unerlässliche Anforderungen für jedes Unternehmen, das einen MDR-Service bewertet, darunter:

- **Kontextbezogene Threat Intelligence:** Nutzung von Threat Intelligence und Bedrohungserkennung in Echtzeit, einschließlich der Korrelation von mehreren Indikatoren, um Bedrohungen zu identifizieren oder falsch positive Ergebnisse zu verwerfen
- **Proaktive Anwendungsfälle:** Unterstützung für die aktive Suche nach bekannten Bedrohungen
- **Umfangreiche Telemetrie:** Ausführung von umfassenden forensischen Ermittlungen und ausgefeilten Analysen, die besonders wichtig für die Identifizierung von neu aufkommenden Bedrohungen sind
- **Korrektur:** Verwendung von kontextspezifischen, KI-gesteuerten Korrekturanleitungen
- **Risikominderung:** Bewertung und Management von Sicherheitslücken

Bei der Auswahl eines MDR-Serviceanbieters sollten Unternehmen nach Partnern suchen, die spezifische und bewährte Funktionen bereitstellen können, wie z. B. die folgenden:

- **24/7-Abdeckung** für kontinuierliches Rund-um-die-Uhr-Monitoring
- **Was-Wenn-Szenarioplanung** und -beratung
- **Menschliches Fachwissen** und Erfahrung seitens des Serviceanbieters
- **Anleitung für** Führungskräfte und Vorstandsmitglieder
- **Gewährleistete Governance**, Compliance und Business Continuity

Zudem sollten Unternehmen die potenziellen MDR-Partner zu den Service-Level-Zielen befragen. Zu diesen Funktionen zählen die durchschnittliche Reaktionszeit (von der Warnmeldung bis zur Initiierung von Ermittlungen), die durchschnittliche Antwortzeit (von der Ermittlungsinitiierung bis zum Zeitpunkt, an dem eine Incident-Analyse für das Unternehmen bereitgestellt wird) sowie die durchschnittliche Lösungszeit (von der Ermittlungsinitiierung bis zum Zeitpunkt der vollständigen Lösung).

Der MDR-Ansatz von Dell Technologies

Für die Auswahl, Bewertung und Zusammenarbeit mit einem MDR-Serviceanbieter ist es erforderlich, dass sich Unternehmen nicht nur auf ihre derzeitigen Anforderungen zur Erkennung von und Reaktion auf Bedrohungen konzentrieren, sondern auch berücksichtigen, wie sich diese Anforderungen in Zukunft entwickeln und erweitern. Natürlich steht keinem Unternehmen eine Kristallkugel für eine Vorhersage von zukünftigen Cybersicherheitsbedrohungen zur Verfügung. Deshalb sollten sie sich für einen MDR-Partner entscheiden, der bereits bewiesen hat, dass er seinen Service im Verlauf der Zeit anhand von innovativer Technologie, bewährten Prozessen und nachgewiesenem Fachwissen durch die MitarbeiterInnen skalieren kann.

Der Ansatz von Dell Technologies für Managed Detection and Response kombiniert flexible, intelligente und skalierbare Technologien mit erfahrenen CybersicherheitsexpertInnen. Der abonnementbasierte Service bietet Unternehmen sowohl planbare Kosten als auch – je nach Bedarf – eine nahtlose Umstellung auf ein höheres Servicelevel.

Die Technologieplattform für Dell Managed Detection and Response ist Taegis XDR, ein vollständig gemanagter, Cloud-nativer Service. Er wurde von Secureworks entwickelt, einer Geschäftseinheit von Dell. Taegis XDR erkennt, analysiert und reagiert auf vollständig geprüfte Bedrohungen, und zwar auf verteilten und unterschiedlichen Angriffsflächen. Die Lösung schützt alle, von großen globalen Unternehmen bis zu relativ kleinen Firmen.

Taegis XDR wird durch die Kompetenzen der zahlreichen SicherheitsanalystInnen und -ingenieurInnen von Dell verstärkt, deren kollektives Fachwissen über Jahrzehnte entstanden ist. So werden Unternehmen vor bekannten und bisher unbekannten Bedrohungen geschützt. Diese Kombination ist eine effiziente Möglichkeit, die Erkennung und Reaktion in der gesamten IT-Architektur zu vereinheitlichen, größtenteils über die kontinuierlich aktualisierte Threat Intelligence-Datenbank. Dell Managed Detection and Response überwacht, analysiert und identifiziert zudem feindliche Verhaltensweisen, um die durchschnittliche Zeit bis zur Erkennung und Reaktion zu verkürzen.

Dell Managed Detection and Response überwacht, analysiert und identifiziert zudem feindliche Verhaltensweisen, um die durchschnittliche Zeit bis zur Erkennung und Reaktion zu verkürzen.

Dell Managed Detection and Response ist ein Managed Service. Damit entfällt für Unternehmen die Notwendigkeit, SicherheitsexpertInnen für bereits überlastete, interne IT- und Sicherheitsbetriebsteams suchen und einstellen zu müssen. Dell Managed Detection and Response ist darauf ausgelegt, die eigenen Funktionen von Unternehmen auf kosteneffiziente, aber strategische Weise zu ergänzen und zu erweitern.

Die ganze Wahrheit

Eine schnell größer werdende Angriffsfläche, wiederholte Ransomwareangriffe und eine allgemein komplexere Bedrohungslandschaft fördern die Investition in XDR- und MDR-Lösungen sowie deren vermehrten Einsatz, da die Unternehmen ihre Programme zur Erkennung von und Reaktion auf Bedrohungen modernisieren. Die einzelnen Sicherheitsstrategien mögen unterschiedlich sein, aber ein umfassender Blick auf die Angriffsfläche sowie die Möglichkeit, große Mengen an Sicherheitsdaten aus den einzelnen Sicherheitskontrollen, die diese schützen, zu aggregieren, zu korrelieren und zu analysieren, ist bei allen ein wichtiger Schritt zur Erlangung der Kontrolle.

Services für Managed Detection and Response sind sowohl effektiv als auch sofort verfügbar, da die Sicherheitsteams MDR-Anbieter zur Förderung von Kompetenzen, Prozessen und Sicherheitstechnologien nutzen. Die ESG-Studie zeigt, dass in XDR investierende Unternehmen zugleich ergänzende MDR-Services wünschen, um diese Lösungen zu implementieren und zu betreiben. Das heißt, sie wenden sich an Lösungsanbieter, die sich bei der Bereitstellung von Sicherheitslösungen und -services bereits bewährt haben. Durch einen langfristigen Einsatz können IT- und Sicherheitsteams im Verlauf der Zeit ihre Sicherheitsprogramme entwickeln und skalieren.

ESG empfiehlt, sich mit MDR-Lösungen von Unternehmen wie Dell Technologies vertraut zu machen. Sie verfügen über die MitarbeiterInnen, Prozesse und Technologien und können Unternehmen bei der Erreichung dieser Ziele unterstützen.

Die Enterprise Strategy Group ist ein integriertes Technologieanalyse-, Forschungs- und Strategieunternehmen, das der globalen IT-Gemeinschaft Marktinformationen, umsetzbare Erkenntnisse und Go-to-Market-Inhaltsdienste bietet.

www.esg-global.com contact@esg-global.com 508.482.0188