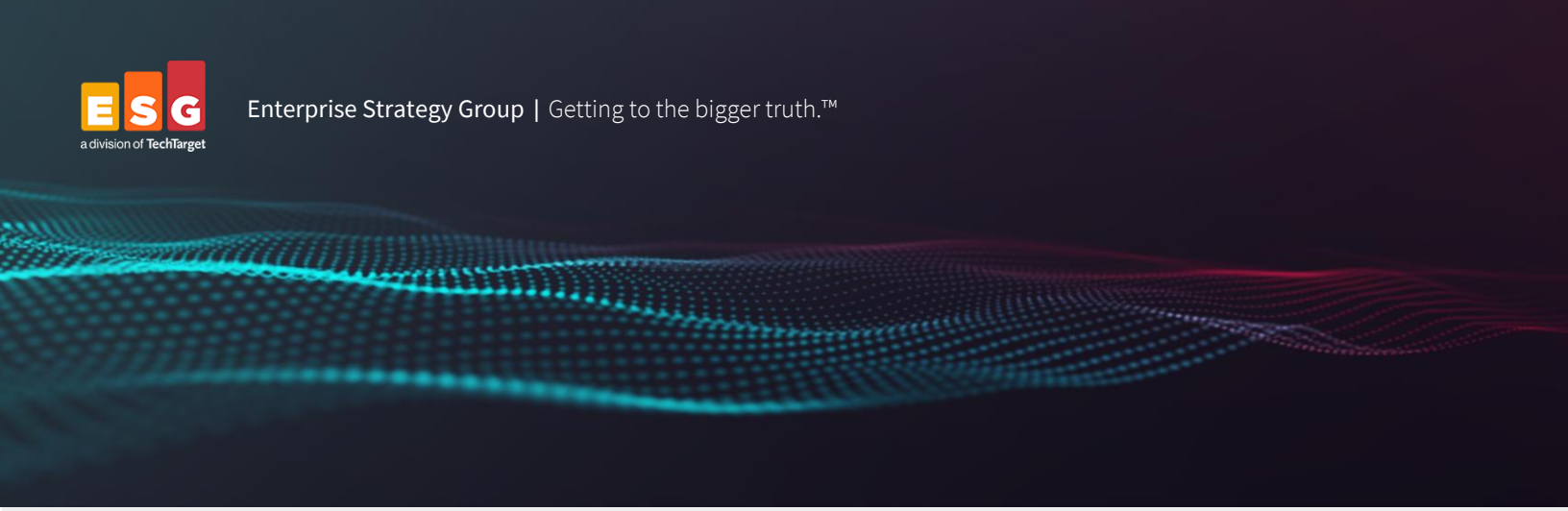


ESG WHITEPAPER

Managed Detection and Response: Ein Weg zum schnellen Ausbau des Sicherheitsprogramms

Von Dave Gruber, Principal Analyst

August 2022

Dieses ESG Whitepaper wurde von Dell Technologies in Auftrag gegeben und wird unter Lizenz von TechTarget, Inc. veröffentlicht.

Inhalt

Kurzfassung

Die Beschleunigung der digitalen Transformation, die schnelle Einführung der Cloud, eine komplexere Bedrohungslandschaft und der anhaltende Fachkräftemangel im Sicherheitsbereich bringen die Sicherheitsteams an ihre Grenzen. Derzeitige Sicherheitslösungen sind nicht in der Lage, Schritt zu halten – das zwingt viele dazu, ihre SOC-Modernisierungsinitiativen zur Neugestaltung von Technologien und Prozessen zu priorisieren. Branchenweite Megatrends rund um Zero Trust und XDR (Extended Detection and Response) bieten eine neue Lösungsvision, allerdings haben viele Schwierigkeiten, die effektiven Implementierungen dieser Strategien effizient zu nutzen und zu operationalisieren. Die Anbieter von MDR(Managed Detection and Response)-Services verfügen über die MitarbeiterInnen, Prozesse und Technologien, sodass zahlreiche Unternehmen ihre Sicherheitsprogramme in dieser turbulenten Umgebung beschleunigen können.

Einführung

Das Risiko von böswilligen Cyberangriffen steigt und zwingt Unternehmen, ihre Priorität und die Budgets von den wichtigsten Geschäftszielen zu verlagern. Sie müssen reagieren und ihre Cybersicherheitsprogramme verstärken. Für einige Unternehmen ist der Aufbau eines vollständigen Sicherheitsprogramms mit internen Ressourcen machbar, die meisten jedoch benötigen Drittanbieterressourcen zur Realisierung eines schnellen Programmausbaus und schneller -skalierung.

Von zentraler Bedeutung für alle Cybersicherheitsprogramme sind Security Operations (SecOps), die für das Monitoring und den Schutz aller Aspekte der digitalen Angriffsfläche verantwortlich sind. Die Einbeziehung von Netzwerken, Endpunkten, Cloud, Identität, Anwendungen und Daten sowie extrem zunehmende Mengen an Sicherheitstelemetriedaten und Warnmeldungen durch SecOps bringen Unternehmen an ihre Grenzen. Als Folge davon wenden sich viele an MDR-Serviceanbieter, um Hilfe zu erhalten.

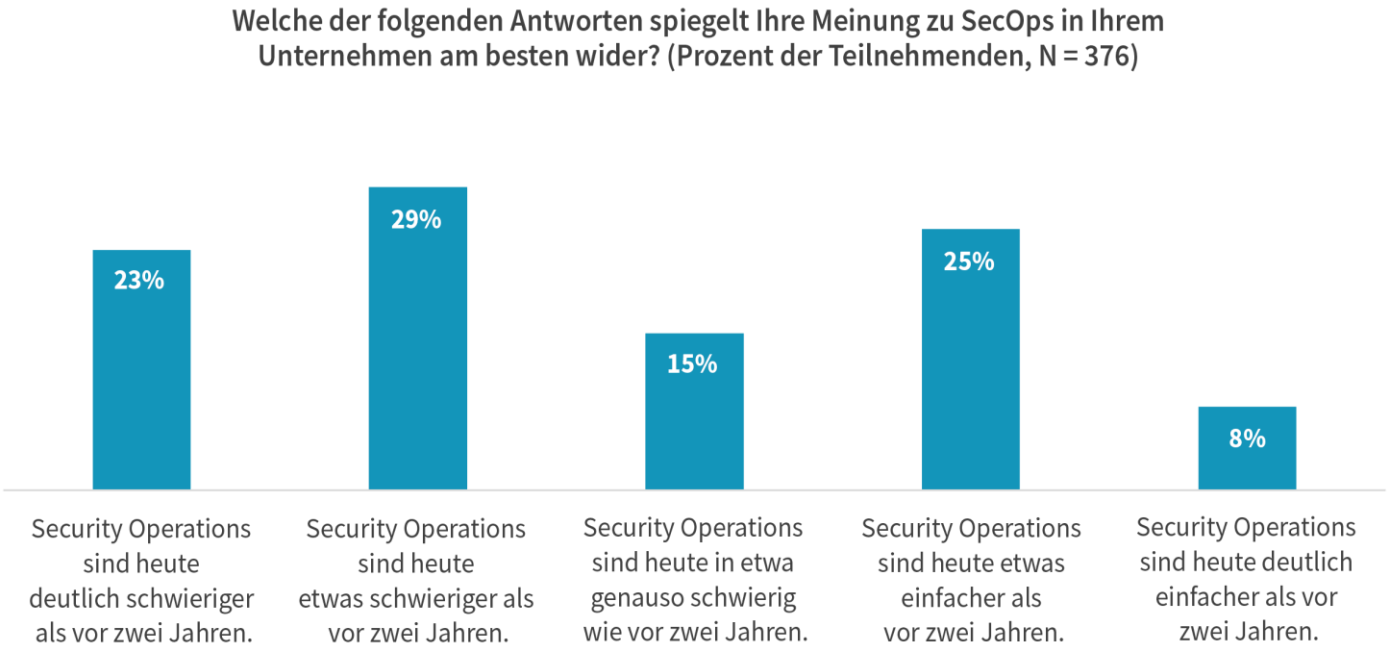
MDR-Serviceanbieter sind zu einem kritischen Mechanismus für diese Unternehmen geworden und bieten etliche Sicherheitsservices, wie z. B. Incident Response, Monitoring rund um die Uhr sowie Programm- und Risikomanagement. Laut einer Studie der Enterprise Strategy Group (ESG) stellen MDR-Services eine Mainstreamkomponente in den modernen Cybersicherheitsstrategien von Unternehmen jeder Größe und mit jeder Sicherheitsstufe dar.

Zunehmend mehr Security-Operations-Herausforderungen

Gemäß einer ESG-Studie (siehe Abbildung 1) sind die meisten Unternehmen der Ansicht, dass die gesamte SecOps-Situation heute schwieriger ist als vor zwei Jahren.[1]

[1] Quelle: ESG Complete Survey Results, *SOC Modernization and the Role of XDR*, August 2022. Alle ESG-Referenzen und -Diagramme in diesem Whitepaper stammen aus diesen Umfrageergebnissen, sofern nicht anders angegeben.

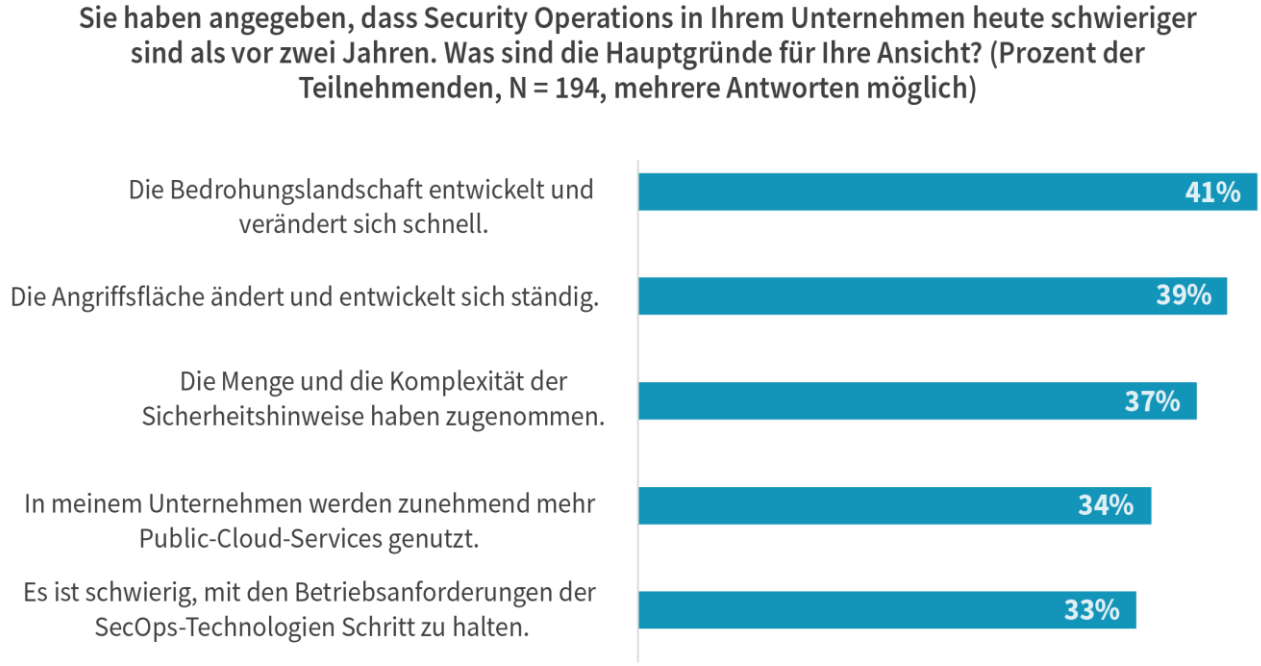
Abbildung 1: Über die Hälfte denkt, dass SecOps schwieriger geworden ist



Quelle: ESG, eine Division von TechTarget, Inc.

Wie in Abbildung 2 dargestellt weist die ESG-Studie auch auf andere Herausforderungen hin, die eine Erkennung und Reaktion schwieriger machen als je zuvor, darunter z. B. die größer werdende Angriffsfläche, die Zunahme und Vielfalt der Bedrohungslandschaft sowie die rasch ansteigende Nutzung von Cloud-Services für eine breitere Palette an Anwendungen und Anwendungsfällen.

Abbildung 2: Die fünf Hauptgründe für die zunehmende Schwierigkeit von SecOps



Quelle: ESG, eine Division von TechTarget, Inc.

Modernisierung von Erkennungs- und Reaktionsprogrammen

Die Angriffsflächen und die Bedrohungslandschaft haben sowohl an Größe als auch an Komplexität zugenommen – ebenso wie der Einsatz von immer mehr Sicherheitskontrollen, die Tausende von Warnmeldungen und enorme Mengen an Sicherheitsdaten erzeugen. Um diese Warnmeldungen und Incidents auswerten und untersuchen zu können, müssen Sicherheitsteams diese Daten aggregieren, korrelieren und analysieren, was häufig einen enormen manuellen Aufwand erfordert. Zudem ist mehr nötig als nur die Erfassung und Analyse von Warnmeldungen und Sicherheitsdaten.

Die Sicherheitsteams überdenken den allgemeinen Programmbetrieb und möchten die Ressourcen- und Risikodaten der IT- sowie der Geschäftsbereichsteams noch enger integrieren, um sich auf die Bedrohungen zu konzentrieren, die das größte Risiko für die Unternehmensziele darstellen. So können z. B. entwendete Zugangsdaten für die Domänenadministration sowohl kurz- als auch langfristig zahlreiche negative Folgen für den Betrieb, die Finanzen und den Markenruf des Unternehmens nach sich ziehen.

Die Sicherheitsverantwortlichen überdenken ihre Strategien und immer mehr Unternehmen outsourcen die täglichen Betriebsaktivitäten an Drittanbieter, weil sich die internen Ressourcen auf strategischere Sicherheitsaktivitäten konzentrieren sollen. Da die internen Sicherheitsressourcen ihren Schwerpunkt auf die Neugestaltung von Security-Operations-Prozessen legen, übernehmen die MDR-Serviceanbieter die Incident-Erkennung, -Bewertung und -Reaktion. Sie ergreifen schnelle Schritte, um Schäden zu vermeiden und potenzielle Betriebsunterbrechungen zu begrenzen.

Andere wenden sich an MDR-Anbieter, um Unterstützung bei der allgemeinen Programmentwicklung zu erhalten und ExpertInnen sowie bewährte Security-Operations-Prozesse zur Optimierung der Ergebnisse einzubeziehen.

Da die XDR-Bewegung weiterhin eine Vision und Roadmap für das schafft, was zur Modernisierung von Erkennungs- und Reaktionsprogrammen erforderlich ist, ziehen andere Unternehmen die MDR-Anbieter zur Unterstützung bei der Implementierung von Lösungen der XDR-Klasse zu Rate.

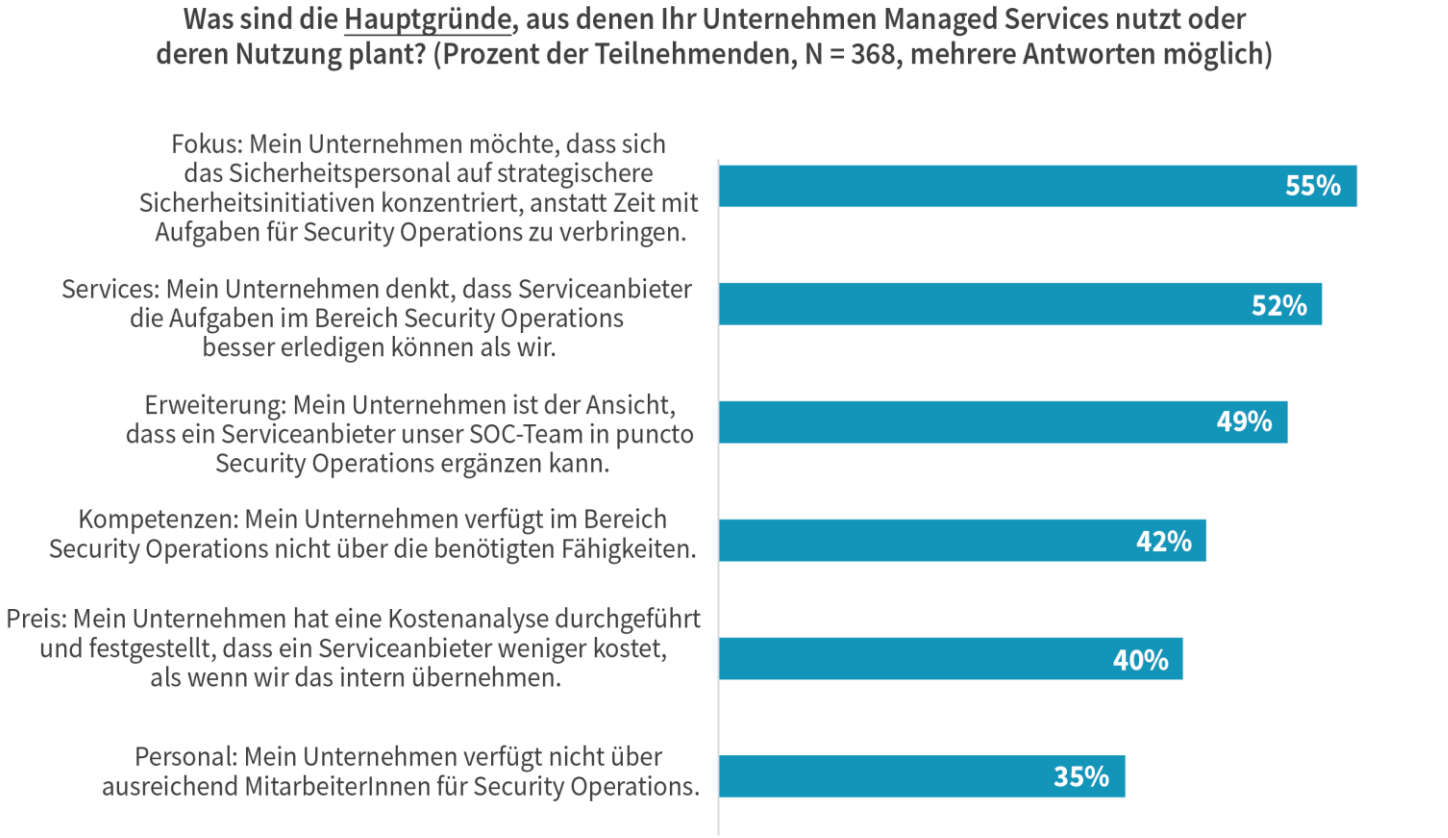
MDR-Anwendungsfälle

Viele MDR-Anbieter bieten zwar zahlreiche Sicherheitsservices an, aber meist beginnen die Projekte mit grundlegenden Erkennungs- und Reaktionsservices für das Monitoring, die Bewertung und die Analyse von Warnmeldungen. Die Betriebsmodelle sind je nach MDR-Anbieter unterschiedlich, sodass die Sicherheitsverantwortlichen die individuellen Anforderungen ihres Unternehmens sorgfältig mit einem MDR-Anbieter abstimmen müssen, der diese spezifischen Ziele erfüllen kann. Einige Sicherheitsverantwortliche entscheiden sich z. B. dafür, ihre Security Operations vollständig auszulagern. Sie arbeiten mit einem MDR-Anbieter zusammen, um die vollständige Abdeckung der Angriffsfläche sowie Bedrohungsmonitoring und Korrekturen zu realisieren. Bei diesem Modell stellen die MDR-Anbieter oft den Technologie-Stack, die Prozesse und die SicherheitsexpertInnen bereit, die für die Serviceerbringung benötigt werden. Andere wiederum betrachten die MDR-Services als Erweiterung ihrer internen SecOps-Funktion, die Abdeckung außerhalb der Geschäftszeiten bietet oder zusätzliche SicherheitsexpertInnen für ein internes Team stellt, das in erster Linie für den Technologie-Stack und den Betriebsprozess verantwortlich ist. Dies sind nur zwei Beispiele für die vielen Anwendungsfälle, in denen MDR-Services genutzt werden.

Folglich ist MDR keine „Universallösung“, sondern eher ein Set an anpassbaren Funktionen, die auf die spezifischen Anforderungen des Unternehmens ausgerichtet werden.

Verschiedene Unternehmen setzen je nach den internen Ressourcen und Kompetenzen unterschiedliche Erkennungs- und Reaktionsschwerpunkte bei der Auswahl ihres MDR-Partners. Die ESG-Studie untersuchte die Hauptgründe dafür in Abbildung 3.

Abbildung 3:Gründe für die Auswahl des MDR-Partners durch Unternehmen



Quelle: ESG, eine Division von TechTarget, Inc.

Wichtige Werttreiber für MDR-Projekte

Für die Entwicklung eines Sicherheitsprogramms ist es erforderlich, den Schwerpunkt auf sowohl Effizienz als auch auf Effektivität zu setzen. MDR-Services können sich auf beides positiv auswirken.

- Betriebliche Verbesserung und Effizienz. Mit MDR können Unternehmen die Gesamtkosten für Security Operations auf verschiedene Weise senken, z. B. bei Infrastruktur, Personal und Management. Außerdem werden Alert-Fatigue (Alarmmüdigkeit) und falsch positive Ergebnisse deutlich reduziert.
- Bessere Cybersicherheitseffizienz und weniger Risiken. Mit MDR können Unternehmen bereits bestehende Bedrohungen stoppen, die Erkennung potenzieller Bedrohungen und erweiterter persistenter Angriffe verbessern, eine proaktive Bedrohungssuche aktivieren und stärkere Kontrollen zur Erkennung und Verhinderung zukünftiger Angriffe einsetzen.

Worauf Sie bei einem modernen MDR-Lösungsanbieter achten sollten

Bedenken Sie, dass MDR-Lösungen im Allgemeinen nicht neu sind. Tatsächlich gibt es sie schon seit einer Weile, mit einer beachtlichen Erfolgsbilanz. Allerdings wurden viele MDR-Lösungen der „Generation 1.0“ für ein anderes Zeitalter mit weniger Daten, weniger Bedrohungen und einfacherer Erkennung entwickelt und implementiert. Die nächste Generation der MDR-Lösungen – und die Drittanbieter, die sie bereitstellen und managen – muss auf breiter gefächerte, tiefergehende und komplexere Herausforderungen ausgerichtet sein, die die Erkennung und Reaktion wichtiger und schwieriger machen als je zuvor.

Bei der Bewertung von MDR-Lösungen sollten Unternehmen auf folgende Funktionen achten:

- 24x7-Monitoring von Ereignissen und Protokollen für die Bereitstellung von schnellen und transparenten Informationen zu verdächtigen Aktivitäten und Warnmeldungen nach Volume, Standort und Typ
- Kontinuierliche und skalierbare Netzwerküberwachung und Bedrohungsanalyse
- KI-gesteuerte Empfehlungen für kontextbezogene Reaktionsoptionen
- Compliancereporting
- „Menschliche“ SicherheitsberaterInnen für den direkten Kontakt zu internen Teams
- Detaillierte Echtzeitanalysen auf Basis von Bedrohungserkennung, -bewertung, -analyse und -forensik
- Anleitungen für Sicherheitslückenbewertungen, Priorisierung und Risikominderung

Angesichts der großen Anzahl potenzieller Serviceanbieter, die einige, viele oder sogar alle outgesourcten MDR-Funktionen bereitstellen können, sollten Unternehmen nach Partnern suchen, die Folgendes bieten:

- Kontextbezogene Threat Intelligence
- Umfangreiche Telemetrie
- Nachweisbare Erfolgsbilanz bei der geografischen Abdeckung, im vertikalen Markt und beim Complianceprofil des Unternehmens
- Nachgewiesene Funktionen für die Bedrohungssuche
- Langfristige Verpflichtung zu Cloud-basierten MDR-Services mit umfangreichen Funktionen für Multi-Cloud- und Hybrid-Cloud-Umgebungen, Zero Trust und dem Modell der geteilten Verantwortung für Cloud-Sicherheit
- Bewiesene Fähigkeit zur Skalierung des Service im Verlauf der Zeit anhand von innovativer Technologie, bewährten Prozessen und nachgewiesenem Fachwissen durch die MitarbeiterInnen

Der MDR-Ansatz von Dell Technologies

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, einem Unternehmen von Dell Technologies. 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.

Die Effizienz von 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 wird als abonnementbasierter Managed Service konfiguriert und bereitgestellt. Damit entfällt für Unternehmen die Notwendigkeit, SicherheitsexpertInnen für die Bewältigung von immer mehr Bedrohungen, Angriffen und Warnmeldungen suchen und einstellen zu müssen. Dell Managed Detection and Response ist darauf ausgelegt, die internen Funktionen von Unternehmen auf effiziente und effektive Weise zu ergänzen und zu erweitern. Als Folge davon haben die internen SecOps-MitarbeiterInnen mehr Zeit und Energie für andere sicherheitsbezogene Aufgaben.

Erfolgsbeispiele: So funktioniert MDR in der Realität

ESG hat mit IT- und SicherheitsexpertInnen von Dell MDR-Kunden gesprochen, um Einblicke in bestimmte Anwendungsfälle, Betriebsmodelle und Ergebnisse zu erhalten.

Beispiel 1: Kommunalbehörde mittlerer Größe

Die IT- und Cybersicherheitsressourcen der Kommunalbehörden entsprechen nur selten denen ihrer KollegInnen im privaten Sektor. Die Probleme, vor denen sie stehen, sind allerdings dieselben. In diesem Beispiel stand ein mittelgroßer Bezirk im Südwesten eines US-Bundesstaates vor der Schwierigkeit, eine wachsende Anzahl von Sicherheitsbedrohungen mit einem sehr knappen Budget bewältigen und lösen zu müssen.

Der neu eingestellte IT-Leiter erkannte sofort die wachsende Bedrohungslandschaft, mit der sein kleines Team konfrontiert war, sowie potenzielle Sicherheitslücken bei dessen Erkennungs- und Reaktionsfunktionen. Er sagte: „Unser Sicherheitsstatus war einfach nicht up to date, aber wir mussten unsere Kompetenzen erweitern, und zwar ohne Mehrkosten bei der Gehaltsabrechnung zu verursachen. Dieses Thema ist für die EntscheidungsträgerInnen der Geschäftsführung sehr wichtig. Aber ich wusste, ich kann die finanziellen Aspekte berücksichtigen und trotzdem auf die Notwendigkeit hinweisen, dass diese Sicherheitslücken geschlossen werden müssen.“

Zunächst bewertete er den vorhandenen Endpoint-Security-Anbieter des Bezirks. Dieser bot dann eine 90-tätige „kostenlose Testversion“ der Softwareupgrades für bessere Erkennung und Reaktion an. Der IT-Leiter stellte jedoch fest, dass die Software ihre Anforderungen nicht erfüllen konnte, außerdem entsprach die Kommunikation mit dem Anbieter nicht seinen Erwartungen. Folglich entschied er sich, auf eine umfassendere MDR-Lösung zu setzen.

„Glücklicherweise hatten wir eine Vereinbarung mit Dell zur Bereitstellung eines virtuellen CSO (Chief Security Officer) getroffen. Die Bezirksleitung kannte also die Vorteile, einen Managed-Services-Ansatz zu nutzen, in diesem Fall für Erkennung und Reaktion." Er fügte hinzu, dass das Dell Team als Ergänzung – und nicht als Ersatz – für das kleine interne Team der Sicherheits- und IT-ExpertInnen im Bezirk fungierte: „Sie waren eine Erweiterung unseres Teams und arbeiteten sehr nahtlos mit unseren MitarbeiterInnen zusammen."

Der wirkliche Vorteil der Vereinbarung trat schnell zutage, als eine globale Hackingkampagne die Web-Mail-Funktion von Microsoft Exchange in Visier nahm. Diese bekannte Plattform wird von zahlreichen Unternehmen, darunter auch von diesem Bezirk. „Sobald Microsoft den Angriff entdeckt hatte, wurde ein Patch entwickelt und bereitgestellt, aber Zero Day für diesen Angriff war vermutlich einen Monat früher", so der IT-Leiter des Bezirks. „Unser virtueller CSO von Dell kontaktierte uns außerhalb der Geschäftszeiten und das Dell MDR-Team sprang ein. Sie sendeten uns Skripte zur Überprüfung des Servers und wir stellten schnell fest, dass einer der Server infiziert war."

„Dell (und ihre Partner von Secureworks) wussten genau, was sie taten. Während der Zeit, in der wir mit dem Angriffsversuch beschäftigt waren, erhielten wir täglich zwei bis drei Anrufe." Er ergänzte, dass das Incident-Response-Team die Ergebnisse mit den MitarbeiterInnen des Bezirks besprach, ihnen Codebeispiele und andere Hinweise auf den Angriff sowie den Beweis für die Kompromittierung zeigte.

Schließlich gaben sie zahlreiche technische und andere Empfehlungen, die nicht nur auf die potenziellen Folgen des Angriffsversuchs ausgerichtet waren, sondern auch das Cybersicherheitsprofil des Bezirks breiter fächerten und langfristig stärkten.

„Unserer Erfahrung nach geht es bei der Suche nach einer besseren Erkennungs- und Reaktionslösung darum, einen zuverlässigen, bewährten und vertrauenswürdigen MDR-Spezialisten zu finden, der sich bereits damit auskennt, anstatt zu versuchen, eine kostengünstige Möglichkeit für ein Upgrade der EDR-Software zu finden". Er sagt: „Ich hatte nicht nur im Nachgang des Angriffsversuchs, sondern auch bei der regelmäßigen Zusammenarbeit mit ihnen das gute Gefühl, dass wir ein tolles Team zu unserem Schutz haben."

Beispiel 2: Schulbezirk mittlerer Größe

Schulbezirke haben in der Vergangenheit stets zu wenig in IT im Allgemeinen und speziell in Cybersicherheit investiert. Aber da Ransomware- und andere Cyberangriffe auf Schulbezirke zunehmen, versuchen die Verantwortlichen bei den Schulbehörden bessere, zuverlässigere und erschwingliche Möglichkeiten zum Schutz vor Sicherheitslücken zu finden.

Beispielsweise wurde ein mittelgroßer US-Schulbezirk per Ransomware angegriffen, dabei wurden alle technologiegesteuerten Vorgänge heruntergefahren. Der Bezirk hatte 8.500 Studierende und MitarbeiterInnen, die auf über 21 Einrichtungen verteilt waren. Er wies ein angemessenes IT-Profil mit 100 physischen Servern und weiteren 63 virtuellen Servern auf, die mit mehr als 11.000 Geräten der Studierenden und MitarbeiterInnen verbunden waren. Offensichtlich bot dieser Bezirk viele potenzielle Einstiegspunkte für böswillige AkteurInnen und benötigte einen Partner, der schnell handeln konnte.

Nachdem der Ransomwareangriff als echte Bedrohung erkannt wurde, der sofortige Maßnahmen erforderte, kontaktierte das IT-Team des Schulbezirks Dell Managed Detection and Response. „Am 2. Tag des Angriffs waren 10 Personen von Dell hier", erinnert sich die IT-Leitung des Bezirks. „Wir hatten eine sehr vertrauenswürdige Beziehung zum Team bei Dell und sie haben sich sofort um das Problem gekümmert."

Glücklicherweise gab es ein positives Ergebnis für den Schulbezirk: „Von den über 6 Millionen Dateien auf unseren Systemen haben wir nur sechs verloren“, sagt die IT-Leitung. „Und die BedrohungsakteurInnen haben wir nie bezahlt. Wir haben bewiesen, dass wir einen Ransomwareangriff überstehen und unsere Arbeit weiterhin sicher und geschützt erledigen können.“

„Die Zusammenarbeit mit Dell war eine positive Erfahrung. Unsere SicherheitsanalystInnen vor Ort sind nach den Gesprächen mit den Dell MitarbeiterInnen immer zufrieden. Unsere Einstellung hat sich im Vergleich zu vor der Zusammenarbeit mit Dell bei Managed Detection and Response um 95 % verbessert.“

Die ganze Wahrheit

Das Risiko von böswilligen Cyberangriffen steigt und zwingt Unternehmen, ihre Priorität und die Budgets von den wichtigsten Geschäftszielen zu verlagern. Sie müssen ihre Cybersicherheitsprogramme verstärken. Die Anwendungsfälle variieren zwar, aber die meisten nutzen MDR-Serviceanbieter, um ihre Programme auszubauen und zu skalieren.

MDR-Serviceanbieter bieten einen Weg, um viele der bekannten Herausforderungen beim Aufbau eines erfolgreichen Sicherheitsprogramms zu überwinden, z. B. durch SicherheitsexpertInnen, bewährte Prozesse sowie skalierbare, einfach bereitzustellende Sicherheitstechnologien.

Dell Technologies verfügt über einen Satz umfassend integrierter Technologien sowie über erfahrene SicherheitsexpertInnen und Best Practices und kann Unternehmen so dabei unterstützen, Bedrohungen nahezu in Echtzeit zu erkennen und darauf zu reagieren. Wie die Fallstudien in diesem Whitepaper zeigen, hat Dell Technologies bereits zahlreichen Unternehmen aus verschiedenen Branchen und mit unterschiedlichen Ressourcenprofilen geholfen, sodass neue Bedrohungen für das gesamte Unternehmen vereitelt werden konnten.

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