Managed Detection & Response (MDR)

Ein Technologie-Ratgeber für mittelständische Industrieunternehmen

Inhaltsverzeichnis

Der Schutz vor Ransomware-Angriffen hat oberste Priorität

Die schnelle digitale Transformation im Fertigungssektor hat eine einzigartige Umgebung geschaffen, die ebenso einzigartige Herausforderungen für die Cybersicherheit mit sich bringt.

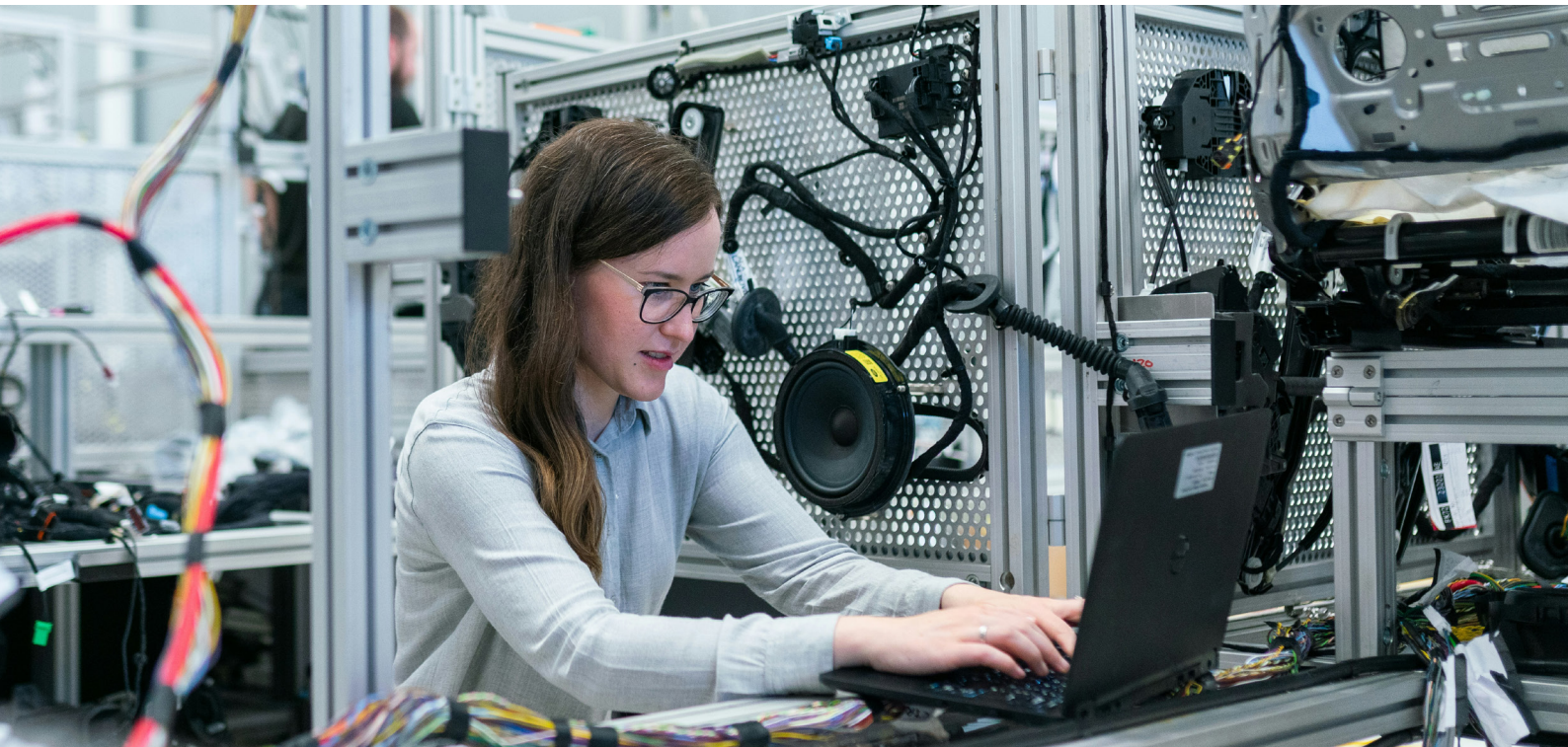
Die häufigste Cyber-Bedrohung für die Fertigungsindustrie unterscheidet sich kaum von anderen Branchen: Ransomware.

26%

ALLER CYBERANGRIFFE ZIELEN AUF HERSTELLER AB

71%

ALLER CYBERANGRIFFE AUF HERSTELLER WAREN RANSOMWARE



Warum brauchen Sie MDR?

Als Hersteller arbeiten Sie in einzigartigen Technologie- und Geschäftsumgebungen. Das macht Sie zu einem attraktiven Ziel für Cyberkriminelle. Der Schutz der Informationen, die die Angreifer für ihre Zwecke missbrauchen wollen, hat für Sie oberste Priorität.

Die traditionellen Sicherheitskontrollen zur Abwehr von Cyberangriffen sind oft unwirksam gegenüber neuen und sich weiterentwickelnden Ransomware-Bedrohungen. Aus diesem Grund werden die verfügbaren Technologien ständig weiterentwickelt.

Dabei handelt es sich vor allem um Technologien, die die Erkennung von und die Reaktion auf laufende Angriffe verbessern.

Um effektiv zu sein, benötigen Erkennungs- und Reaktionswerkzeuge eine kontinuierliche Überwachung und den Einsatz von fachkundigem Sicherheitspersonal (Security Operations, SecOps). MDR-Dienste wurden entwickelt, um Unternehmen zu entlasten und ihnen den Aufbau eines eigenen Sicherheitsteams zu erleichtern. In diesem Leitfaden finden Sie eine Übersicht über die Möglichkeiten zur Auslagerung Ihrer SecOps-Kompetenzen.

> **"MDR-Dienste bieten Kunden eine von Experten geführte und schlüsselfertige SOC-Lösung der nächsten Generation, die speziell darauf ausgelegt ist, Bedrohungen effektiv zu erkennen und einzudämmen."**
>
> **— Gartner**

Das Wichtigste an dieser Definition ist der Begriff „von Experten geführt". MDR-Anbieter können aufgrund ihrer Skalierbarkeit eine Dienstleistung zu niedrigeren Kosten erbringen, als dies durch Insourcing möglich ist. Die MDR-Dienste unterscheiden sich jedoch erheblich, und viele bieten nicht die von Gartner erwähnte schlüsselfertige Komplettlösung.

Machen Sie die Erkennung und Reaktion auf Bedrohungen zu einer Priorität?

Nach Angaben des Weltwirtschaftsforums werden 4 Millionen Fachkräfte benötigt, um den Fachkräftemangel in der globalen Cybersicherheitsbranche zu schließen. Diese Zahl könnte bis 2030 auf 85 Millionen steigen.

Nur die größten Industrieunternehmen haben das Budget für die Einstellung des gesamten IT- und Sicherheitspersonals, das für die Umsetzung und Verwaltung eines ausgereiften Sicherheitsprogramms erforderlich ist. Die Unternehmen, die über diese Möglichkeiten verfügen, haben immer noch mit der Herausforderung zu kämpfen, die richtigen Mitarbeiter zu finden und zu behalten.

Im Folgenden erläutern wir, welche Maßnahmen Sie ergreifen können, um Ihre Sicherheitslage zu verbessern, damit Sie schnell auf einen Cyberangriff reagieren, ihn eindämmen und die Sicherheit Ihrer Systeme wiederherstellen können. Als Verantwortlicher für die IT-Sicherheit ist es Ihre Aufgabe, die Vorteile und Herausforderungen jedes Ansatzes abzuwägen und denjenigen auszuwählen, der den Bedürfnissen Ihres Unternehmens am besten entspricht.

Outsourcing und Partnerschaften - drei wichtige Optionen

Informations- und Cybersicherheitsmaßnahmen erfordern viele verschiedene Teams und Mitarbeiter. Bei der Evaluierung von Anbietern sollten Sie die folgenden Bereiche berücksichtigen und festlegen, welche davon vorrangig sind:

- Governance, Risk and Compliance (GRC)
- Bewertung von Sicherheitsrichtlinien, Architektur und Technologie
- Security Operations mit einem Schwerpunkt auf der Erkennung von und Reaktion auf Vorfälle

Im Folgenden werden die drei wichtigsten Outsourcing-Optionen vorgestellt:

	VORTEILE	NACHTEILE
Auslagerung einiger Aspekte der IT- und Cybersicherheit Viele Unternehmen entscheiden sich dafür, einige Elemente ihrer Sicherheitsprogramme auszulagern und andere intern fortzuführen.	Sie haben weniger Aufwand, eigene Mitarbeiter einzustellen. Sie können an Experten und spezialisierte Unternehmen auslagern, die wettbewerbsfähige Preise anbieten. Bietet Flexibilität bei der Auswahl der Funktionen, die Sie auslagern möchten. Ermöglicht die Auslagerung taktischer Maßnahmen während strategische Bereiche im Unternehmen bleiben.	Die Pflege einer Vielzahl von Partnerschaften, z. B. mit einem virtuellen CISO (vCISO), Beratungsunternehmen, Beratern und Managed Security Service Providern (MSSP). Hohe Gesamtbetriebskosten (TCO) - Kosten für die Einrichtung und Verwaltung einer komplexen „Lieferkette“, die Risiken mit sich bringt: • Wer ist für welche Teile Ihrer Sicherheitsstrategie zuständig? • Mangelnde Klarheit über Rollen und Zuständigkeiten • Die Verwaltung mehrerer Service Level Agreements (SLAs) führt zu einem hohen Verwaltungs- und Managementaufwand.
Auslagerung der Überwachungs-maßnahmen an einen MSSP (Managed Security Service Provider) Ein MSSP bietet die Fernüberwachung von Sicherheitslösungen und die Reaktion auf Vorfälle von seinem SOC aus.	Es ist nicht mehr erforderlich, ein SOC aufzubauen oder ein SecOps-Team zu beschäftigen. Sie können dies an Experten und spezialisierte Unternehmen auslagern. Die Erkennungs- und Reaktionsmaßnahmen werden mit hoher Priorität bearbeitet und entlasten Ihr Team. Sie erhalten eine 24/7-Unterstützung.	Viele der oben genannten Hindernisse gelten auch für diese Variante. Ein MSSP unterstützt möglicherweise nicht alle Ihrer Produkte. Die Überwachung aller Produkte könnte zu kostspielig sein. MSSPs bieten möglicherweise keine Bedrohungssuche und keine vollständige Reaktion auf Vorfälle an. Viele sortieren lediglich Warnmeldungen und leiten Maßnahmen an ihre Kunden weiter. MSSPs helfen Ihnen möglicherweise nicht beim Aufbau Ihrer Sicherheitsstrategie oder bei der Durchführung proaktiver Aktivitäten wie der Verwaltung von Angriffsflächen (ASM) und der Schwachstellenerkennung.
Auslagerung an einen MDR-Anbieter Viele Unternehmen lassen diesen Prozess von einem erfahrenen MDR-Anbieter betreuen.	MDR-Anbieter sind Experten, die sich auf die Verringerung des Risikos eines Vorfalls konzentrieren. Sie unterstützen eine bestimmte Anzahl von Technologien, sodass die Komplexität und die Kosten entfallen, die einem MSSP durch die Verwaltung von Hunderten von Produkten entstehen. Die geringere Komplexität führt zu einer schnellen Installation und einer schnelleren Einführung der Schutzmaßnahmen.	Die Nachteile sind ähnlich wie bei den anderen oben genannten Auslagerungsoptionen. Viele MDR-Anbieter haben sich jedoch auf den Mittelstand konzentriert und schaffen einen erheblichen Mehrwert für ihre Kunden.

Wählen Sie einen MDR-Partner, der Mehrwert für alle strategischen und operativen Aspekte Ihres Sicherheitsprogramms bietet

Es gibt viele Anbieter auf dem Markt, die sehr unterschiedliche Dienstleistungen anbieten – von einfacher Alarmtriage, Ereigniskorrelation und Berichterstattung bis hin zu echten Partnerschaften, bei denen sie zu einer Erweiterung Ihrer IT- und Sicherheitsabteilung werden.

Schlüsselkriterien zur Bewertung von MDR-Anbietern

Die Kriterien zur Bewertung von MDR-Anbietern lassen sich in drei Hauptkategorien einteilen. Dies hilft Ihnen, genau zu verstehen, wie ein Anbieter Sie bei Ihrem End-to-End-Sicherheitsprogramm unterstützen kann.

Verstehen Sie genau, was Sie von Ihrem MDR-Anbieter benötigen, um Ihre Ziele, Ihr Team und Ihre Organisation zu unterstützen.	
Wählen Sie einen Partner und keinen Lieferanten	Suchen Sie nach einem Partner, der eine Erweiterung Ihrer IT- und Sicherheitsteams darstellt und diese befähigt, erfolgreich zu werden. Er sollte anpassungsfähig sein, Ihre Kompetenzlücken schließen und Sie über Ihr gesamtes Sicherheitsprogramm hinweg unterstützen.
Unterstützung in Ihrer lokalen Sprache	Bewerten Sie, wie wichtig Ihnen Support in ihrer Muttersprache ist. Bietet Ihr Anbieter Support auf allen Ebenen während Ihrer Geschäftszeiten? Viele große, internationale Anbieter bieten nur einen lokalen First-Level-Support. Dies kann dazu führen, dass Informationen vom operativen Sicherheitsteam durch mehrere Ebenen weitergeleitet werden müssen, was Verzögerungen und potenzielle Missverständnisse verursacht. Stellen Sie sicher, dass jede benötigte Support-Ebene während Ihrer Geschäftszeiten verfügbar ist.

Datenresidenz	Dies stellt für viele Organisationen eine Herausforderung dar, in manchen EU-Ländern mehr als in anderen. Wenn Informationen die EU verlassen müssen, könnten Risiken der Nichteinhaltung entstehen, die eine Prüfung Ihres Anbieters sowie neue Datenverarbeitungsvereinbarungen erfordern. Weitere Komplexitäten entstehen zudem, wenn bestehende Vereinbarungen mit Partnern in der Lieferkette angepasst werden müssen.
Integriertes Kundenportal	Suchen Sie nach Dienstleistern, die das Risiko von Datenverstößen durch ASM (Attack Surface Management) und proaktives Schwachstellenmanagement mit Unterstützung von Cybersicherheitsexperten verringern. Das Kundenportal Ihres Anbieters sollte Ihnen einen Überblick ihrer Angriffsfläche bieten, mit leicht verständlichen, umsetzbaren Erkenntnissen, damit Sie Ihre Maßnahmen nach Prioritäten ordnen und Risiken verwalten können.
Integrierte Benutzer-befähigung und Sichtbarkeit von Benutzerrisiken	Achten Sie auf Anbieter, die Mehrwerte liefern und Ihre Sicherheitslage durch Benutzertrainings stärken. Regelmäßige Security Awareness Trainings (SAT) und Testprogramme sind nicht nur durch viele Regularien vorgeschrieben, sondern schaffen auch eine Sicherheitskultur im Unternehmen. Das Konzept des menschlichen Risikomanagements gewinnt an Bedeutung. Dies hilft Organisationen, die mit ihren Benutzern verbundenen Risiken zu verstehen. Dabei kann es sich um intrinsische Risiken handeln, die mit ihrer Position in der Organisation und ihrem Zugang zu hochwertigen Vermögenswerten verbunden sind, oder um Risiken, die durch Schulungen ermittelt wurden. SAT sollte idealerweise in das Portal Ihres MDR-Anbieters integriert sein, um eine ganzheitliche Sicht auf Ihre Sicherheitslage zu ermöglichen.
Wertbeitrag nachweisen, um Budgets zu rechtfertigen	Suchen Sie nach einem Anbieter, dessen Berichte und Dashboards dabei helfen, Ihren Sicherheitsaufwand zu rechtfertigen und zusätzliche Budgets freizuschalten. Durch ein klares Verständnis Ihrer Sicherheitslage und deren Entwicklung über die Zeit können Sie die Effektivität des Anbieters messen und Argumente für eine Budgeterhöhung anbringen.
Sicherheits-niveau gegenüber Kunden und Partnern nachweisen	Industrieunternehmen haben eine komplexe Kette von Zulieferern und Kunden, die sich im Rahmen eines Onboarding-Prozesses gegenseitig überprüfen. Suchen Sie einen Anbieter, der diesen Prozess vereinfacht und verkürzt, indem er es Ihnen ermöglicht, nachzuweisen, dass Ihr Sicherheitsprogramm ausgereift und Ihr Unternehmen widerstandsfähig ist und dass Sie sich selbst im schlimmsten Fall eines erfolgreichen Angriffs schnell wieder erholen können.

Erkennung und Reaktion

Verringern Sie das Risiko einer Datenverletzung oder eines erfolgreichen Ransomware-Angriffs, indem Sie Angriffe erkennen, eindämmen und darauf reagieren.	
Proaktive Unterstützung	Ihr Ziel sollte über die bloße Reaktion auf Vorfälle hinausgehen. Ein Anbieter, der hilft, Schwachstellen zu managen, reduziert das Risiko erfolgreicher Angriffe. Wenn ein Angreifer dennoch eindringt, können Angriffe durch ein fundiertes Verständnis Ihrer IT-Umgebung, Benutzer und kritischen Vermögenswerte verlangsamt und eingedämmt werden.
Schnelle Reaktion ermöglichen	Suchen Sie nach einem technologieneutralen Anbieter, der flexibel ist und die besten Technologien verwendet, um sich schnell an neue Bedrohungen anzupassen. Der Anbieter sollte eigene Anwendungen und Tools integrieren, um Lücken zu schließen und die Reaktionszeit zu verkürzen.
Schnellere implementierung und Mehrwert	Wenn Ihr Anbieter sein Technologieangebot effektiv gestaltet hat, kann er einen Großteil der Implementierung und Integration in Ihre Umgebung automatisieren und so die Zeit bis zur Nutzung des Dienstes verkürzen. So profitieren Sie schneller von den Diensten des Anbieters.
Umfassende Abdeckung	Ein Anbieter sollte nicht nur als reines Alarmsystem agieren. Ein guter Anbieter sollte eine vollständige Reaktion auf Angriffe durchführen, inkl. Bedrohungssuche, Eindämmung und Unterstützung bei der Wiederherstellung.
Transparente Leistungsmetriken	Stellen Sie sicher, dass Anbieter SLAs einhalten und quantifizierbare Metriken liefern, welche die Leistung und den Erfolg ihrer Dienstleistungen belegen.
Bericht über den Mehrwert der Lösung	Sie müssen in der Lage sein, den Mehrwert von gebündelten oder zusätzlichen Funktionen und Diensten zu demonstrieren. Dies sollte allen Beteiligten in verständlicher Form über ein Portal oder einen Bericht mitgeteilt werden.

Wiederherstellung und Cyber-Versicherung

Im Falle eines Angriffs – Was kann Ihr MDR-Anbieter tun, um Risiken und finanzielle Schäden zu mindern?	
DFIR, Ursachen-analyse und Beratung	Ihr Anbieter sollte über DFIR-Fähigkeiten (Digital Forensics and Incident Response) im eigenen Haus verfügen, um das MDR-Team bei der Ursachenanalyse innerhalb der vereinbarten SLAs zu unterstützen und über den gesamten Lebenszyklus eines Vorfalls zu berichten, von der ersten Eindringung bis zur finalen Eindämmung. Er sollte Beratung sowie optional praktische Expertise anbieten, um Ihnen bei der Behebung und Wiederherstellung nach einem Vorfall zu helfen.
Ransomware-Verhandlungen	Unternehmen sollten nicht ohne Expertenrat einfach Lösegeld zahlen oder unvorbereitet versuchen, den Angreifer zu kontaktieren. Um die besten Chancen auf eine erfolgreiche Wiederherstellung Ihrer Daten zu haben, selbst wenn Sie sich entscheiden zu zahlen, benötigen Sie die Unterstützung eines spezialisierten Verhandlungsführers. Einige Anbieter verfügen über diese Expertise.
Beziehen Sie Cyber-Versicherungen von einem MDR-Anbieter	Fertigungsunternehmen erkennen die Bedeutung von Cyber-Versicherungen. Verschiedene Faktoren treiben dies voran, darunter regulatorische Anforderungen, die Anforderungen von Partnern entlang der gesamten Lieferkette und die Minderung der finanziellen Risiken, die mit Betriebsunterbrechungen verbunden sind.
Vereinfachen Sie den Antrags-prozess für Versicherungen	Versicherer müssen Ihr Sicherheitsniveau bewerten, um das Risiko einer Versicherung einzuschätzen. Wenn Sie Ihre Versicherung von einem Anbieter beziehen, der proaktiv mit Versicherungsunternehmen zusammenarbeitet und dessen Dienstleistungen überprüft wurden, kann dies die Anzahl der Fragen, die Sie beantworten müssen, oft um bis zu 80 % reduzieren.
Reduzieren Sie Kosten	MDR-Anbieter, die Versicherungen über Partner-Versicherer anbieten, sollten proaktiv Rabatte für alle ihre Kunden ausgehandelt haben. Diese können zwischen 25 % und 35 % liegen.
Vereinfachte Verlängerung	Zusätzlich zum vereinfachten Erst-Antragsprozess sollte auch die Verlängerung problemlos und unkompliziert ablaufen.

Wählen Sie Ihren MDR-Anbieter-Typ sorgfältig aus

Ihre erste Entscheidung besteht darin, festzulegen, auf welcher grundlegenden Technologie die Erkennung und Reaktion basieren soll. Dazu stehen Ihnen die folgenden drei Lösungen zur Verfügung:

- Endpoint detection and response (EDR)
- Network detection and response (NDR)
- Extended detection and response (XDR)

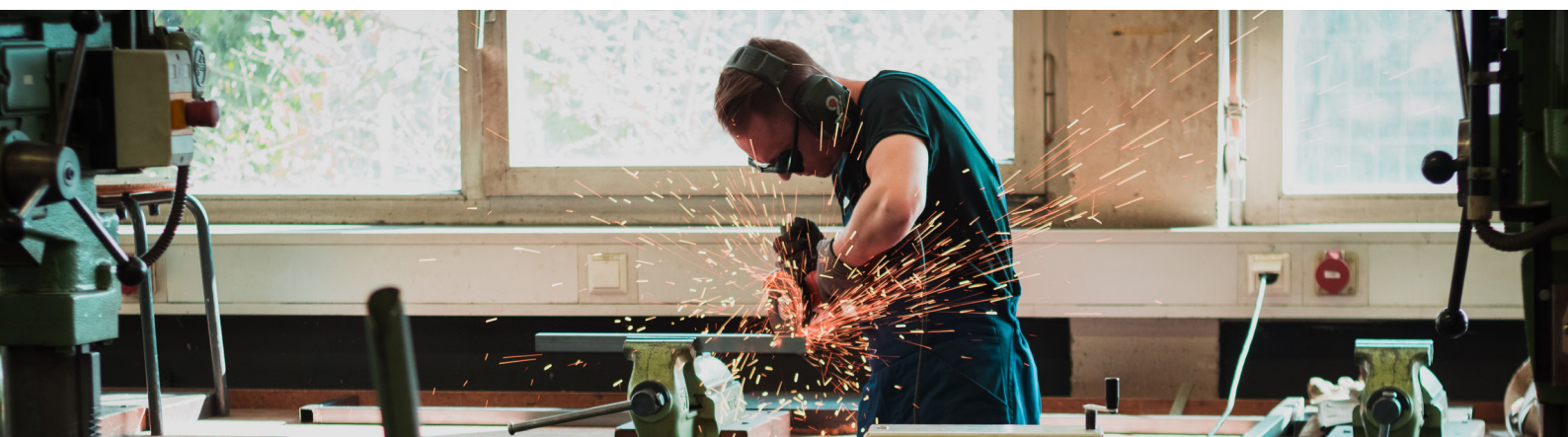
Die meisten MDR-Anbieter bieten eine Komponente von XDR an und bezeichnen ihren Dienst häufig als MXDR. Sie verarbeiten Ereignisse aus punktuellen Sicherheitsmaßnahmen und korrelieren diese mit Ereignissen von EDR oder NDR. Typischerweise bildet eine dieser beiden Technologien die Grundlage der MXDR-Dienstleistung und wird mit der anderen Technologie angereichert. Ihre Entscheidung besteht also darin auszuwählen, welche der Beiden grundlegenden Technologien Sie bevorzugen.

NDR wird häufig als die bessere Wahl für Fertigungsbetriebe empfohlen, da es den gesamten Netzwerkverkehr, einschließlich des Verkehrs von Betriebstechnologien, kontinuierlich überwacht und Produktionssysteme häufig nicht mit einem EDR ausgestattet werden können. Wenn jedoch der Schutz vor Ransomware Ihre oberste Priorität ist, könnte EDR die bessere Wahl sein. Denn um Daten zu verschlüsseln oder zu stehlen, muss ein Angreifer zuerst ein verwaltetes Gerät wie einen Laptop, Server oder Computer kompromittieren – ein Bereich, in dem EDR besonders effektiv ist.

Unabhängig davon, welche Technologie Sie bevorzugen, müssen Sie nun den MDR-Anbieter-Typus auswählen, der am besten zu Ihren Anforderungen passt.

ANBIETER-TYP	VORTEILE	HERAUSFORDERUNGEN
Anbieter von Endpoint-, Cloud- und Netzwerksicherheitssoftware (dienstleistungspaket direkt vom Anbieter)	Experten für ihre eigene Technologie. Globale Abdeckung mit mehreren SOCs (Security Operations Centers), die Rund-um-die-Uhr-Support bieten.	Unterstützen ausschließlich ihre eigenen Produkte; wenig bis keine Korrelation von Warnmeldungen über mehrere Kontrollpunkte hinweg, um eine schnelle Priorisierung und Reaktion zu ermöglichen. Hauptfokus liegt auf großen, multinationalen Unternehmenskunden.
Große MDR-Anbieter und Telekommunikationsunternehmen/ große MSSPs (Managed Security Service Providers)	Experten für die Vielzahl der Produkte, die sie unterstützen. Globale Abdeckung mit mehreren SOCs, die oft Rund-um-die-Uhr-Support bieten.	Die Unterstützung einer Vielzahl von Technologien führt zu langsamer Integration und Servicebereitstellung. Eingeschränkte Möglichkeiten zur Vorfallreaktion und Wiederherstellung; oft unflexibel. Hauptfokus liegt auf großen Unternehmenskunden.
Lokale MDR-Anbieter	Typischerweise sind sie spezialisiert und verfügen über Experten für die von ihnen unterstützte Produktpalette, was eine schnelle Bereitstellung und Reaktion ermöglicht. Flexible Geschäftspartner mit einem hohen Maß an Service-Orientierung und Wertschöpfung. Lokale Sprache und Datenresidenz.	Unterstützt möglicherweise nicht alle Produkte in Ihrer Umgebung.

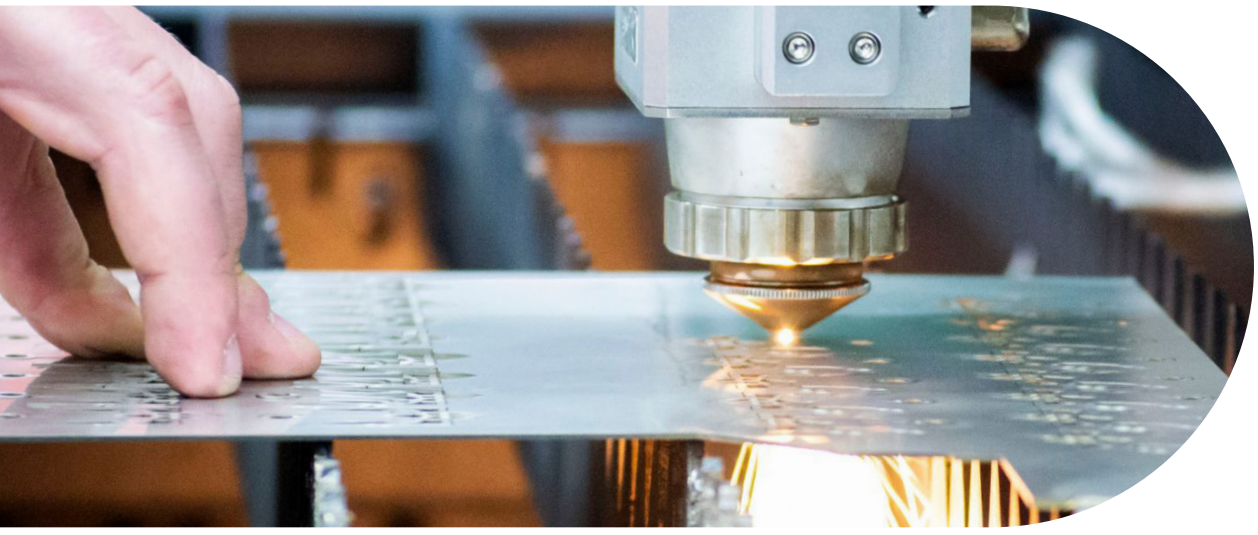
In einem Markt mit vielen Auswahlmöglichkeiten ist es entscheidend, genau zu verstehen, was MDR-Anbieter anbieten, damit Sie Lücken identifizieren und dadurch sehen, was durch interne Ressourcen abgedeckt werden muss. Selbst wenn ein Anbieter behauptet, alle Ihre Anforderungen abzudecken, sollten Sie klären, was im Basispaket enthalten ist und was zusätzliche Kosten verursacht.



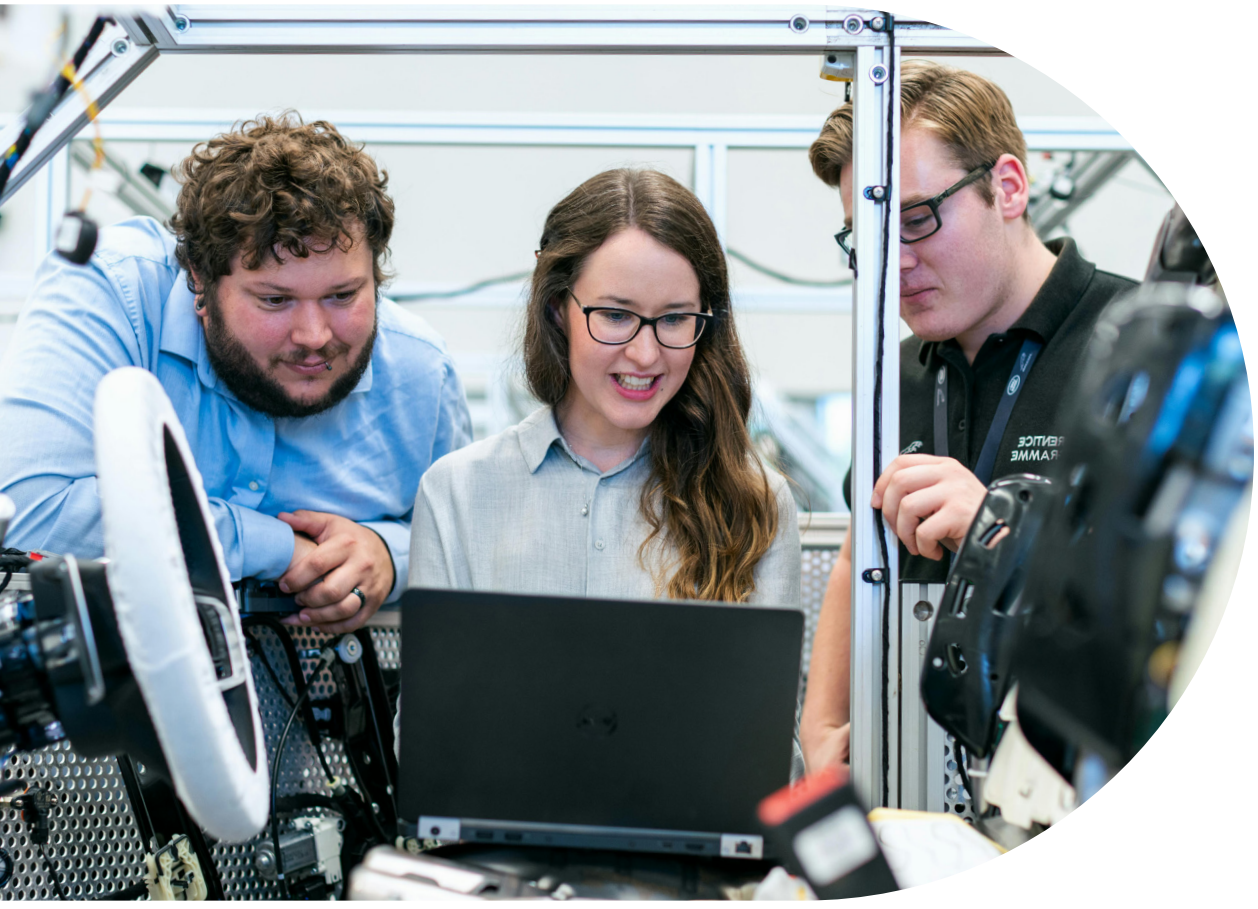
Mit diesen Fragen finden Sie den richtigen MDR-Anbieter

Enablement	
Lokaler Kundensupport	• Bieten Sie Rund-um-die-Uhr-Support in der Landessprache an? • Werden meine Daten in einem anderen Land verarbeitet?
ASM* und Schwachstellen-management	• Ist Angriffsflächemanagement (Attack Surface Management, ASM) im Angebot enthalten? • Bieten Sie die Erkennung digitaler Assets und Benutzer/Identitäten an? • Erfolgt Ihr Erkennungsprozess zu einem bestimmten Zeitpunkt oder wird er kontinuierlich in regelmäßigen Abständen aktualisiert? • Ist die Schwachstellensuche enthalten? • Handelt es sich um punktuelle Scans, z. B. alle drei Monate, oder kontinuierliche Scans, z. B. täglich oder wöchentlich? • Bieten Sie Beratung zum Schwachstellenmanagement an? • Überwachen Sie Domänen, Hosts und Gerätekonfigurationen auf Schwachstellen und geben Empfehlungen zur Verbesserung der Sicherheit ab? • Bieten Cybersicherheitsexperten Beratung zu Erkenntnissen über Angriffsflächen an? Wie werden diese präsentiert?
SAT und Sichtbarkeit der Risiken durch Benutzer	• Bieten Sie Sichtbarkeit über alle meine Benutzer? • Bieten Sie eine Cybersicherheitsschulung (Security Awareness Training, SAT) an? • Ist die SAT-Berichterstattung in Ihr Kundenportal integriert, sodass ich neben anderen Informationen eine zentrale Übersicht über das Benutzerrisiko erhalte?
Berichte	• Gibt es ein Kundenportal, das alle Bereiche der Serviceleistung sowie die Reaktion auf Vorfälle abdeckt?
Von Experten erbrachte Leistungen	• Ist Expertenrat für alle Bereiche der Serviceleistung sowie für die Reaktion auf Vorfälle enthalten? • Bieten Sie einen VCISO*-Service? (*Ein virtueller CISO).

Erkennung und Reaktion	
ASM und Schwachstellen-management	• Nutzen Sie die während des ASM-Prozesses gesammelten Informationen, um die Erkennung und Reaktion zu erleichtern?
SOC-Werkzeuge	• Verlassen Sie sich nur auf Werkzeuge von Drittanbietern oder verfügen Sie über eigene, integrierte Technologien, um eine schnelle Reaktion in allen unterstützten Umgebungen zu ermöglichen?
Reaktions-prozess	• Korrelieren Sie Warnmeldungen und untersuchen Vorfälle, um ihre Priorität zu bestimmen? • Ergreifen Sie Maßnahmen, um einen Angriff einzudämmen? Welche Maßnahmen bieten Sie? • Beispielsweise - Für Geräte– Beenden eines Prozesses oder Isolieren eines Endpunkts - Für Cloud -Anwendungen – Deaktivieren von Benutzerkonten, Widerrufen von Sitzungen oder Erzwingen einer Kennwortzurücksetzung
Berichte und Kommunikation	• Wie sieht der Kommunikationsprozess während eines Vorfalls aus? • Welche Informationen stellen Sie nach der Vorfallbehandlung zur Verfügung?
SLAs und Kennzahlen	• Welche Service Level Agreements (SLAs) bieten Sie? • Wie dokumentieren Sie deren Einhaltung?



Wiederherstellung und Cyberversicherung	
Berichte	• Bieten Sie eine Ursachenanalyse an, die den gesamten Lebenszyklus eines Vorfalls beleuchtet? • Stellen Sie Empfehlungen bereit, um das Risiko ähnlicher Vorfälle zu minimieren? • In welcher Form werden diese Empfehlungen bereitgestellt?
Cyberver-sicherung	• Haben Sie Partnerschaften mit Versicherungsanbietern? • Wie wirkt sich Ihre Leistung auf Versicherungsprämien aus? Vereinfacht der Abschluss über Ihre Versicherungspartner den Antrags- und Erneuerungsprozess?
Von Experten erbrachte Leistungen	• Können Sie beratende Unterstützung während der Wiederherstellungsphase anbieten? • Unterstützen Sie bei Verhandlungen im Falle eines Ransomware-Angriffs?



Fallstudien

KeyTec Niederlande

Als die Berichte über Ransomware in der Branche immer häufiger wurden, beschloss das Fertigungsunternehmen KeyTec Netherlands, Maßnahmen zu ergreifen. Erfahren Sie, wie Eye Security das Unternehmen dabei unterstützt hat, seine Abwehrkräfte proaktiv zu stärken und eine Sicherheitskultur zu schaffen.

Signature Foods

Da die Internetkriminalität immer raffinierter wird, wenden sich Unternehmen vermehrt an externe Anbieter. Erfahren Sie, wie Eye Security Signature Foods in nur wenigen Wochen zu einem umfassenden Cyberschutz verholfen hat.

„Die Zeitungsberichte über Unternehmen, die von Ransomware betroffen waren, nahmen zu, ebenso wie die Bedrohung durch digitale Angriffe. Unser CFO verlangte mehr Einblick in unseren Sicherheitsstatus. Als wir dann auch noch Anfragen von einigen wichtigen Kunden erhielten, wie wir sicherstellen, dass ihre Daten bei uns sicher sind, wurde uns klar, dass es an der Zeit war, unseren aktuellen Sicherheitsstatus kritisch zu überprüfen."

— Rik Jaeken
IT-Manager, KeyTec

„Dass die Mitarbeiter von Eye Security Anomalien in unserem Netzwerk erkennen und Vorfälle schnell identifizieren können, beruhigt mich sehr. Eye Security hat sich bereits bewährt."

— Peter Onland
IT-Manager, Signature Foods

Bei Eye Security konzentrieren wir uns auf die Grundlagen, priorisieren die Endpunktsicherheit und setzen die Netzwerküberwachung gezielt ein, um Lücken zu schließen. Auf diese Weise ermöglichen wir die Entwicklung einer robusten Sicherheitsstruktur, die Angreifern immer einen Schritt voraus ist und auf neue Bedrohungen reagieren kann.

www.eye.security