Cybersecurity Checkliste: Zehn Auswahlkriterien für MDR-Services

Wie Managed Detection and Response (MDR) Sicherheits-Verantwortliche in der Industrie beim Aufbau einer zukunftsfähigen Sicherheitsarchitektur unterstützt

Skyline Obrela, Bilder © Obrela

Autor:
Stefan Bange
Managing Director Germany
Obrela
www.obrela.com

Die Bedrohungslage in der Cybersecurity verändert sich rasant und trifft immer stärker auch die fertigende Industrie. Angreifer richten dabei Taktiken, Techniken und Prozesse (TTPs) gezielt auf Schwachstellen in Produktions- und Fertigungsbetrieben aus. Das Problem: Statt ganzheitlichem Sicherheitsansatz finden sich in vielen Unternehmen inkohärente Sicherheitslösungen. Managed Detection and Response (MDR) stellt diesem Flickenteppich einen holistischen, permanenten und dynamischen Schutzansatz gegenüber. Die Cybersecurity-Experten von Obrela zeigen, worauf es bei der Auswahl von MDR-Services ankommt.

Managed Detection and Response Services

Der Markt für MDR-Lösungen wächst stark: Laut dem Gartner Market Guide for Managed Detection and Response Services (2024) ist die Marktdurchdringung (Mind Share) im Jahresvergleich um 29,14 % gestiegen, während die Adoption von MDR-Services zwischen 2021 und 2022 um 67 % zulegte. Diese Dynamik unterstreicht den zunehmenden Bedarf an fortschrittlicher Bedrohungserkennung und -abwehr. Gleichzeitig stehen Security-Verantwortliche vor einer unübersichtlichen Vielfalt an Anbietern. Um fundierte Entscheidungen treffen zu können, müssen Hersteller eine strukturierte Auswahl treffen.

Wesentliche Merkmale eines effektiven MDR-Partners

Ein leistungsfähiger MDR-Service erkennt nicht nur Bedrohungen in klassischen IT-Umgebungen, sondern adressiert auch spezifische Risiken in Fertigungs- und Produktionsanlagen, analysiert und reagiert aktiv auf Vorfälle. Wichtige Unterscheidungsmerkmale sind dabei: die Kombination aus KI-gestützter Analyse und menschlicher Expertise, die Fähigkeit zur aktiven Bedrohungsabwehr in Echtzeit, vollständige Transparenz über alle sicherheitsrelevanten Bereiche (Endpunkte, Cloud, OT, IoT) sowie die Skalierbarkeit des Angebots. Ebenso entscheidend ist die Nachvollziehbarkeit durch klar definierte Kennzahlen, individualisierbare Berichte und transparente Zuständigkeiten.

MDR-Checkliste: Zehn zentrale Fragen

1. **Gibt es ein durchgängig besetztes 24/7-SOC?**
   Ein echtes 24/7-Security Operations Center (SOC) ist durchgängig mit qualifizierten Analysten besetzt, auch nachts und an Wochenenden. Ein „Follow-the-Sun"-Modell sollte auf Konsistenz, Übergabeprozesse und Erfahrungsniveau der Teams genau geprüft werden. Entscheidend ist, ob auch außerhalb der Geschäftszeiten erfahrene Sicherheitsanalysten eigenständig Fälle bewerten und bearbeiten können.

2. **Wie strukturiert und transparent ist der Onboarding-Prozess?**
   Ein effektiver Onboarding-Prozess umfasst mehrere Phasen: von der Projektplanung über die technische Integration bis hin zur Konfiguration, Datenvalidierung und einem abschließenden Funktionstest. Transparenz entsteht durch klar definierte Meilensteine, etwa zur Installation von Agenten, zur Log-Ingestion und zur Simulation realistischer Angriffsszenarien. Die Begleitung durch einen dedizierten Projektmanager sollte Teil des Leistungsumfangs sein.

3. **Wie steht es um Governance-, Risiko- und Compliance-Anforderungen?**
   Ein leistungsfähiger MDR-Anbieter bietet nicht nur Sicherheitsüberwachung, sondern unterstützt auch bei der Einhaltung gesetzlicher und regulatorischer Anforderungen. Dazu zählen beispielsweise Compliance-Reports für NIS2 oder GDPR, GAP-Analysen, unterstützende Audits sowie Vorlagen für Sicherheitsrichtlinien und Risikomanagement-Prozesse.

4. **Was sind die konkreten Incident-Response-Fähigkeiten?**
   Die Reaktionsfähigkeit bei Sicherheitsvorfällen ist ein zentrales Kriterium – besonders in Fertigungsprozessen, wo Produktionsausfälle durch Cyberangriffe erhebliche wirtschaftliche Folgen haben können. Ein klar definierter Übergabeprozess vom SOC an ein Incident Response Team sowie regelmäßig getestete Eskalationsmechanismen sind Voraussetzung. Ausschlaggebend ist auch, wie viele Stunden Incident-Response-Leistung im Leistungsumfang enthalten sind und ob sich mit den Services bzw. Ressourcen auch mehrere Vorfälle parallel abdecken lassen.

5. **Lassen sich im Ernstfall eigenständig Remote-Maßnahmen zur Eindämmung umsetzen?**
   Eine zentrale Anforderung bei MDR ist es, bei bestätigten Sicherheitsvorfällen sofortige Maßnahmen einzuleiten. Dazu zählen unter anderem Netzwerkisolation, das Beenden kompromittierter Prozesse, das Sperren von Benutzerkonten oder das Blockieren schädlicher Verbindungen, idealerweise über integrierte EDR- oder XDR-Plattformen. Ein abgestimmter Autorisierungsprozess stellt sicher, dass Maßnahmen rechtssicher und kontrolliert ablaufen.

6. **Was sind die Mechanismen zur Erkennung von Zero-Day-Bedrohungen?**
   Die Reaktion auf Zero-Day-Bedrohungen – etwa gezielte Angriffe auf industrielle Steuerungssysteme (ICS) – erfordert eine Kombination aus maschineller Erkennung und menschlicher Bewertung. Neben kontinuierlich aktualisierten Detection-Rules sind auch verhaltensbasierte Analysen (Behavioral Analytics) und Bedrohungsmodellierung erforderlich. Die Nutzung spezifischer Threat-Intelligence-Feeds, die auch „never-before-seen"-Indikatoren enthalten, ist hierbei von besonderer Bedeutung.

7. **Wie gut und aktuell sind die genutzten Threat-Intelligence-Quellen?**
   Entscheidend für die Wirksamkeit eines MDR-Dienstes ist nicht die Anzahl, sondern die Relevanz und Aktualität der verwendeten Bedrohungsdaten. Hochwertige Anbieter greifen auf eine Kombination aus kommerziellen Quellen, Open-Source-Plattformen wie MISP und eigenen Research-Teams zurück. Zusätzlich ist eine aktive Beteiligung an Community-gestütztem Informationsaustausch – etwa über ISACs oder ENISA-Kanäle – ein Indikator für hohe Qualität.

8. **Wie umfassend ist die Überwachung von MDR?**
   Ein ganzheitlicher MDR-Ansatz bietet vollständige Transparenz über klassische IT-Infrastrukturen, Cloud-Umgebungen, mobile Arbeitsplätze, IoT-Komponenten und industrielle Steuerungssysteme (OT). Die Integration erfolgt idealerweise über APIs, Agenten, syslog oder cloud-native Konnektoren. Eine anschließende Daten-Normalisierung und die Ereigniskorrelation in Echtzeit bilden die Grundlage für eine ganzheitliche Sicherheitsüberwachung.

9. **Ist die Abdeckung von industriellen OT-Umgebungen im MDR-Service integriert?**
   Insbesondere in kritischen Infrastrukturen und Fertigungsumgebungen ist die Absicherung von Operational Technology (OT) essenziell. MDR-Anbieter sollten über Erfahrung mit OT-Protokollen verfügen und passive Überwachungstechniken, wie etwa Deep Packet Inspection, anwenden können. Eine einheitliche Triage und Analyse über IT- und OT-Grenzen hinweg ist für eine koordinierte Reaktion auf hybride Bedrohungen erforderlich.

10. **Lassen sich die MDR-Services nahtlos in bestehende Sicherheitstechnologien integrieren?**
    Ein moderner MDR-Dienst sollte sich ohne tiefgreifende Infrastrukturänderungen in bestehende Sicherheitsarchitekturen integrieren lassen. Dazu gehört die Kompatibilität mit etablierten SIEM-, EDR-, IAM- und CMDB-Lösungen. Neben einer vollständigen Schnittstellenübersicht (API, Agent, syslog, native Integration) ist es wichtig, dass bidirektionale Kommunikation unterstützt wird und Prozesse zur laufenden Pflege und Aktualisierung definiert sind.

Kurz zusammengefasst

„Die MDR-Checkliste bietet einen guten Startpunkt für den Vergleich von Anbietern, besonders für Hersteller, die ihre Produktionssysteme und vernetzten Fertigungsanlagen besser absichern wollen. Die Auswahl des passenden MDR-Partners ist jedoch keine Standardentscheidung", erklärt Stefan Bange, Managing Director Germany bei Obrela. „Der richtige Fit hängt stark vom individuellen Risikoprofil und den konkreten Anforderungen des Unternehmens ab. Branchenspezifische Rahmenbedingungen, gesetzliche Vorgaben wie GDPR oder NIS2, die Komplexität der bestehenden IT-Landschaft sowie die internen Sicherheitskapazitäten spielen dabei eine entscheidende Rolle. Am Anfang steht deshalb immer eine systematische Bestandsaufnahme der eigenen Sicherheitsanforderungen und der strategischen Ziele. Nur so lässt sich sicherstellen, dass MDR-Services nicht nur technische Anforderungen erfüllen, sondern langfristig zu einer tragfähigen und wirksamen Sicherheitsstrategie beitragen."

Wer schreibt:

Obrela ist ein weltweiter Anbieter von Cybersicherheitsdiensten. Das Unternehmen bietet Services rund um Sicherheitsanalytik und Risikomanagement, um ausgeklügelte Bedrohungen in Echtzeit zu identifizieren, zu analysieren, vorherzusagen und zu verhindern. 2010 gegründet, unterstützt Obrela beim Echtzeit-Cyber-Risikomanagement und kombiniert dabei Threat Detection and Response (MDR) mit Managed Risk and Controls (MRC) Services. ◄

Link

Die Checkliste für die Auswahl von MDR-Services mit weiteren Kriterien und Details finden Sie im kostenlosen Whitepaper „20 Critical Questions to Identify the Right MDR Provider for Your Business" auf der Obrela Webseite. https://www.obrela.com/whitepaper/is-your-business-truly-protected-20-questions-to-ask-before-choosing-an-mdr-provider/