Fully Managed- versus Co-Managed-Detection & Response Service

Welchen Service braucht die IT Security?

Unternehmen können ihre IT Security wegen Fachkräftemangels oft kaum aufrechterhalten – und die Bedrohungen wachsen durch immer raffiniertere Angriffsformen. Hier kann die individuelle Inanspruchnahme von IT-Sicherheits-Services nach dem Baukastenprinzip mit flexiblen, hybriden Ansätzen helfen: Co-Managed Detection und Response Services schließen bei fehlenden Ressourcen, Expertise oder Fachkräften Lücken in der Cyberabwehr und stellen eine wertvolle Alternative zu kompletten Inhouse-Konzepten oder Fully Managed Services dar.

Eine leistungsstarke IT Security stützt sich grundsätzlich auf zwei Säulen: einerseits auf die Verhinderung oder zumindest die Verlangsamung erfolgreicher Cyberangriffe durch umfangreiche Sicherheitsmechanismen, andererseits auf eine schnelle Erkennung und Abwehr von Cyberangriffen, welche die Sicherheitsmechanismen umgehen konnten. Je weiter die Digitalisierung voranschreitet, desto herausfordernder wird es, Unternehmen vor Schäden durch Cyberangriffe zu schützen: Raffiniert aufgebaute Malware, Ransomware, bösartige Skripte und Advanced Persistent Threats (APTs), die meist mittels Social Engineering den Weg ins Netzwerk finden, bedrohen die IT-Sicherheit von Unternehmen weltweit.

In den letzten Jahren hat sich dabei eine Tendenz verstärkt, die mittlerweile zu einer der größten Gefahren für die Cyberabwehr geworden ist: Es fehlt an notwendiger Manpower; der Fachkräftemangel schlägt auch in der IT Security Branche voll durch. Vor allem kleinere und mittlere Unternehmen können freie Stellen nur schwer besetzen. Spezialisierte IT-Sicherheitsdienstleister bieten hier mit Managed Detection & Response (MDR) Services die dringend benötigte Unterstützung. Diese zusätzliche, externe Manpower entlastet unternehmensinterne IT Security-Teams bzw. bietet Unternehmen die Möglichkeit, über ein „eigenes“ IT Security-Team zu verfügen.

Was bedeutet Detection & Response?

Der alleinige Einsatz klassischer Sicherheitsmaßnahmen gewährleistet längst keine wirkungsvolle IT Security mehr. Heute zählen eine schnelle und umfassende Gefahrenerkennung und -abwehr mehr denn je. Dafür setzen bereits viele Unternehmen unterschiedlichste „Threat Detection and Response“ Tools ein, die das Ziel haben, Angriffsaktivitäten zeitnah aufzuspüren, zu melden und teilautomatisiert abzuwehren: EDR (Endpoint Detection & Response), NDR (Network Detection & Response) oder XDR (Extended Detection & Response) gelten derzeit

als relevante sicherheitstechnische Lösungen, die aktuellen und zukünftigen Cyberbedrohungen wirkungsvoll gegenüberstehen.

Hinter den jeweils drei Buchstaben von EDR, NDR oder XDR verbergen sich zusammenfassend „Detection and Response"-Technologien, die Cyberangriffe detektieren, also erkennen, und diese in unterschiedlicher Ausgestaltung managen. Die Lösungen werden eingesetzt, um Angriffe auf Unternehmensnetzwerke frühzeitig zu erkennen und schnellstmöglich zu stoppen.

Verantwortliche IT Security Teams – zumeist Cyber Defense Analysten und Threat Hunter – erhalten durch Detection & Response Lösungen umgehend Meldungen über identifizierte Auffälligkeiten sowie sicherheitsrelevante Daten, die auf akute Bedrohungslagen hinweisen. Damit werden sie in die Lage versetzt, in kürzester Zeit angemessen zu reagieren und großen Schaden abwehren zu können.

Warum Managed Detection & Response Services?

Einer groß angelegten, globalen Studie zufolge gefährdet fehlende Manpower in 85 Prozent aller Unternehmen die Cybersicherheit. Entlastung auf dem Arbeitsmarkt ist nicht in Sicht, im Gegenteil: Alle Indikatoren weisen darauf hin, dass sich das Problem in den nächsten Jahren nochmals deutlich verschärfen wird. Managed Detection & Response Services (MDR) setzen genau an dieser eklatanten Schwachstelle an. Der Begriff steht für die verwaltete Erkennung und Reaktion von Angriffen. Hier steht nicht die Technologie oder eine Lösung im Vordergrund, sondern ein Service, der von spezialisierten IT Security Dienstleistern wie SECUINFRA bereitgestellt wird.

Unternehmen können damit auf Dienstleistungen von professionellen IT Security-Providern zurückgreifen, die auf die Erkennung, Analyse und Abwehr von Cyberangriffen spezialisiert sind – idealerweise rund um die Uhr. So kann der für ein Unternehmen extern verantwortliche IT Security Analyst beispielsweise mithilfe eines Orchestrierungs-Tools (Security Orchestration Automation and Response, kurz: SOAR) bei Erkennung und Bestätigung einer realen Bedrohung umgehend entsprechende Abwehrmaßnahmen in die Wege leiten. Die MDR-Leistungen können je nach Bedarf in Anspruch genommen werden und entlasten interne IT-Sicherheitsteams von Routineaufgaben oder der zeitintensiven Bearbeitung von Fehlalarmen.

Fully Managed oder Co-Managed-Service?

Ein Fully Managed Detection & Response Service ist als Komplettpaket zu verstehen, bei dem alle für ein Unternehmen notwendigen bzw. sinnvoll erachteten IT Security Tools von einem Service Provider zur Verfügung gestellt, verwaltet und betrieben werden. Hierbei kann es sich zum Beispiel um ein SIEM (Security Information and Event Management) handeln, ergänzt um

ein SOAR-System zur schnelleren, teilweise automatisierten Analyse und Abwehr von Cyberangriffen. An SIEM und SOAR sind alle Systeme angebunden, die einen potenziellen IT-Sicherheitsvorfall initial erkennen, weitere Informationen zur Beurteilung liefern oder Schutzmaßnahmen einleiten können. Konkret kann es sich dabei etwa um die Anbindungen von EDR/NDR/XDR Lösungen handeln. Es können aber auch weitere Lösungen wie Phishing Detection, Threat Intelligence oder Vulnerability Management angebunden werden.

Security Service Provider führen beim Fully MDR Service die Implementierung und den Betrieb aller benötigten IT Security Tools durch und überwachen die Netzwerke und Endgeräte der Kunden auf Anomalien rund um die Uhr an sieben Tagen in der Woche. Bei Bedarf werden Abwehrmaßnahmen in enger Absprache mit dem Kunden in die Wege geleitet. Zusätzlich werden alle anfallenden administrativen Arbeiten wie das Auswerten von Logfiles, die Aktualisierung der eingesetzten Tools mit Patches und Updates oder die Erstellung von Berichten vom Dienstleister übernommen.

Ein Co-Managed Detection & Response Service zeichnet sich durch eine individuelle und flexible Inanspruchnahme aus: Betrieb und Verwaltung bestimmter Security Tools werden auf einen Service-Provider übertragen. Der Co-Managed Ansatz basiert dabei auf der Tatsache, dass viele Organisationen und Unternehmen bereits in IT Security Tools wie AntiPhishing, SIEM, EDR/NDR/XDR und SOAR investiert haben, dann aber feststellen mussten, dass ein lückenloser, effizienter Betrieb an ausreichend Manpower scheitert. Fehlende Expertise oder zusätzliche Tools lassen sich bei Co-Managed Detection & Response Services nach dem Baukastenprinzip hinzubuchen – mit planbaren, transparenten und skalierbaren Kosten.

Wissenstransfer und enge Zusammenarbeit

Co-Managed Detection & Response Services sind dabei nicht als Ersatz, sondern als Ergänzung zur bestehenden IT-Sicherheitsarchitektur zu sehen, um sicherzustellen, dass auf identifizierte IT-Sicherheitsbedrohungen umgehend und angemessen reagiert werden kann. Dank der Expertise und Manpower des MDR Service Providers gelingt das so schnell, dass maßgeblicher Schaden vom Unternehmen abgewendet oder zumindest stark reduziert werden kann. Darüber hinaus bieten Co-Managed Detection & Response Services noch einen weiteren, nicht zu unterschätzenden Vorteil: Die Kunden erhalten hochwertige Beratungsleistungen und einen Wissenstransfer. Denn eine enge Zusammenarbeit ist maßgeblicher Teil von Co-Managed-Serviceansätzen. Erfahrene, externe Spezialisten kompensieren das fehlende Expertenwissen im Unternehmen – und die unternehmensinterne IT profitiert durch den fachlichen Austausch von deren Know-How.

Fazit

Erfahrene Fachkräfte im Bereich der IT Security sind auf dem Arbeitsmarkt kaum zu bekommen. Vor allem kleine und mittlere Unternehmen stehen allzu häufig ohne die dringend benötigte menschliche Expertise dar, selbst wenn technische Security Lösungen vorhanden sind. Managed Detection & Response (MDR) Services füllen diese Lücken in der Cyberabwehr. Während Fully Managed Detection & Response Services als Komplettpaket alle notwendigen Tools und Leistungen bereitstellen, gleichen modular und flexibel aufgebaute Co-Managed Detection & Response Services fehlende Ressourcen und Kapazitäten in bestimmten Bereichen gezielt aus.

Autoren:

Ramon Weil - Founder & CEO - SECUINFRA GmbH
Norbert Nitsche - Head of Cyber Detection & Response Center - SECUINFRA GmbH

Weitere Informationen: https://www.secuinfra.com/de/techtalk/fully-managed-versus-co-managed-detection-response-welchen-service-braucht-ihre-it-security/

Pressekontakt:

SECUINFRA GmbH
Svenja Koch
Stefan-Heym-Platz 1
10367 Berlin
Deutschland
Tel. +49 (0) 160 921 633 44
svenja.koch@secuinfra.com