MDR-Leitfaden: Schützen Sie Ihr KMU mit einer digitalen Alarmzentrale vor Cyberangriffen

Was ist ein MDR und wie erhöht es die Sicherheit?

Ein MDR (Managed Detection and Response) oder SOC (Security Operations Center) fungiert als digitale Alarmzentrale, die darauf ausgelegt ist, die gesamte IT-Infrastruktur eines Unternehmens kontinuierlich zu überwachen und vor Hackerangriffen zu schützen. Durch diese kontinuierliche Überwachung können Bedrohungen in Echtzeit erkannt und analysiert werden, was es ermöglicht, Sicherheitsvorfälle frühzeitig zu identifizieren und zu verhindern.

Viele MDR/SOC-Dienstleister arbeiten dabei rund um die Uhr und nutzen fortschrittliche Technologien zur frühzeitigen Erkennung und aktiven Verhinderung von Bedrohungen. Dabei werden sicherheitsrelevante Daten aus Endpunkten, Netzwerken, Clouddiensten und Identitäten zentral korreliert, um Bedrohungen kontextbasiert zu erkennen, automatisiert darauf zu reagieren und sie bereits im Vorfeld durch integrierte Präventionsmechanismen aktiv zu verhindern.

Sobald eine Bedrohung erkannt wird, wird ein erfahrenes Team von Sicherheitsexpertinnen und -experten alarmiert. Dieses Team im Bereitschaftsdienst hat die Aufgabe, schnell und effektiv auf erkannte Sicherheitsvorfälle zu reagieren. Massnahmen zur Schadensbegrenzung und Wiederherstellung werden aus der Ferne vom Expertenteam eingeleitet, um Auswirkungen auf den Geschäftsbetrieb zu verhindern oder zu reduzieren.

Durch die Kombination aus fortschrittlicher Technologie und menschlichem Fachwissen bietet ein MDR/SOC-Dienst ein hohes Mass an Sicherheit. Er minimiert das Risiko von Schäden durch Cyberangriffe und trägt erheblich zur Erhöhung der Sicherheit und Stabilität der IT-Systeme eines Unternehmens bei. Dies ist besonders wichtig in Zeiten, in denen Cyberbedrohungen immer komplexer und häufiger werden.

Welche Unternehmen sollten sich mit MDR schützen?

Es ist pauschal schwierig zu beurteilen, welche Unternehmen sich mit einem MDR schützen sollten, da dies stark vom individuellen Risikoappetit und den spezifischen Bedürfnissen abhängt. Insbesondere grössere KMU mit schützenswerten Daten oder hoher IT-Abhängigkeit sollten eine MDR-Implementierung in Betracht ziehen. Der Schweizerische Versicherungsverband empfiehlt Unternehmen mit 30 oder mehr PC-Arbeitsplätzen eine Auseinandersetzung mit diesem Thema.

Generell jedes Unternehmen sollte prüfen, inwieweit der beauftragte IT-Dienstleister sich um die Überwachung der Systeme kümmert und wie es um die Reaktionsfähigkeit bei Hackerangriffen steht. Ist ein IT-Dienstleister oder an einen ausgelagerten MDR-Dienstleister nicht explizit mit diesen Funktionen beauftragt, können Angriffe womöglich nicht erkannt und nicht abgewehrt werden.

Was sollte eine sinnvolle MDR-Implementierung können?

Eine sinnvolle MDR-Implementierung sollte auf die spezifischen Bedürfnisse und Anforderungen des Unternehmens zugeschnitten sein. Es gibt unterschiedliche Varianten einer MDR-Lösung, die von grundlegenden Funktionen bis hin zu umfassenden, fortschrittlichen Sicherheitsmassnahmen reichen.

In der Schadenprävention hat sich gezeigt, dass sich das Risiko mit einem guten Kosten-Nutzen-Verhältnis schrittweise reduzieren lässt. Im Folgenden werden drei Varianten beschrieben: Die Basisvariante zum Einstieg, eine Standardvariante und eine Variante für den umfassenden Schutz. Jede dieser Varianten bietet unterschiedliche Grade an Schutz und Funktionalität, um den jeweiligen Anforderungen gerecht zu werden.

– **Basisvariante: Aufbau präventiver Schutzmechanismen**

  Installation eines verhaltensbasierten Endpoint-Detection-and-Response(EDR)-Agenten auf Laptops und Servern sowie Integration von Identitätsdaten aus dem Active Directory und von Firewall-Alarmen. Der EDR-Agent ist ein moderner Antivirenschutz, der in einigen Fällen Angriffe automatisiert blockieren kann. Er ersetzt in vielen Szenarien oft die bereits installierte Antivirensoftware.

– **Standardvariante: Sicherstellung der Handlungsfähigkeit bei Angriffen**

  Etablierung eines Reaktionsprozesses, der rund um die Uhr auf sicherheitsrelevante Ereignisse reagieren kann und die EDR- bzw. Sicherheitsmeldungen auswertet. Dabei ist entscheidend, dass der MDR-Dienstleister über ein IT-Notfallteam verfügt, um im Ernstfall fachgerecht zu intervenieren. Je nach Risikoprofil sollte das IT-Notfallteam die Sicherheitsmeldungen rund um die Uhr und auch an Wochenenden überwachen. In vielen Fällen reicht eine Abdeckung werktags während der Bürozeiten.

– **Umfassende Variante: Erweiterung der Sichtbarkeit und Szenarienabdeckung**

  Etablierung eines Erkennungssystems, welches Meldungen aus zusätzlich angebundenen Alarm- und Überwachungssystemen auswertet und auf welches das IT-Notfallteam Zugriff hat. Beispielsweise können zusätzlich Meldungen von Applikationen oder Clouddiensten eingebunden werden, um kundenspezifische Erkennungsszenarien abzubilden und die Sicherheitslage weiter zu verbessern.

Wie hoch ist der finanzielle Aufwand?

Die Kosten für eine MDR-Implementierung können stark variieren und hängen von verschiedenen Faktoren ab. Einer der Hauptfaktoren ist die zeitliche Abdeckung und das gewünschte Service Level, also ob eine Überwachung rund um die Uhr oder nur während bestimmter Zeiten erfolgt. Auch die Menge der verarbeiteten Daten und die Anzahl der Quellen spielen eine Rolle bei der Preisgestaltung. Eine bestehende EDR-Installation und Microsoft-Defender-Lizenzierung können den Preis für die Überwachung ggf. reduzieren. In der Regel fallen Kosten pro Monat und pro überwachtem PC-Arbeitsplatz und Server an, die sich im Rahmen von 10 bis 15 Prozent des IT-Budgets bewegen.

Was muss man bei der Beauftragung beachten?

Bei der Beauftragung eines MDR-Dienstes gibt es mehrere wichtige Aspekte zu beachten. Zunächst sollte geprüft werden, ob der eigene IT-Dienstleister den MDR-Service als Reseller anbietet. Dies kann den Implementierungsprozess vereinfachen und sicherstellen, dass der Dienst nahtlos in die bestehende IT-Infrastruktur integriert werden kann. Falls nicht Microsoft Defender verwendet wird, ist die Installation eines entsprechenden Agenten erforderlich, und es muss sichergestellt werden, dass die Firewall so konfiguriert ist, dass Alarme zugelassen und verarbeitet werden können. Ein weiterer wichtiger Punkt ist die enge Zusammenarbeit des MDR-Dienstleisters mit dem bestehenden IT-Dienstleister, um eine schnelle Reaktion und Isolation bei erkannten Bedrohungen zu gewährleisten. Diese Zusammenarbeit ist entscheidend für die Effektivität der Sicherheitsmassnahmen und die Minimierung von Schäden durch Cyberangriffe.

Welche Anbieter gibt es in der Schweiz?

Beispiele für in der Schweiz tätige Anbieter, die sich auf MDR/SOC spezialisiert haben:

- Adnovum
- Axians
- Compass Security
- InfoGuard
- Inseya
- Kudelski Security
- Netaccess
- Netcloud
- Swisscom
- Wizlynx

Fazit

Ein Managed-Detection-and-Response(MDR)-Dienstleister bietet Unternehmen einen umfassenden Schutz vor Cyberbedrohungen durch kontinuierliche Überwachung und schnelle Reaktion auf Sicherheitsvorfälle. Angesichts der zunehmenden Komplexität und Häufigkeit von Cyberangriffen ist der Einsatz von MDR-Diensten für Unternehmen jeder Grösse und Branche von grosser Bedeutung. Der Schweizerische Versicherungsverband SVV empfiehlt Unternehmen, sorgfältig die passenden MDR-Anbieter auszuwählen und die spezifischen Bedürfnisse und Risiken zu berücksichtigen. Eine gut implementierte MDR-Lösung kann wesentlich zur Erhöhung der Cyberresilienz und damit zur Sicherheit und Stabilität der gesamten IT-Infrastruktur beitragen.

Was ist der SVV?

Der Schweizerische Versicherungsverband SVV ist die Branchenorganisation der Schweizer Privatversicherer. Der Verband setzt sich für eine nachhaltige Entwicklung der Versicherungswirtschaft ein und fördert Lösungen, die zur Stabilität und Sicherheit der Schweizer Wirtschaft und Gesellschaft beitragen. Ein wesentliches Ziel des SVV ist es, Schweizer Unternehmen sicherer zu machen. Durch seine Aktivitäten trägt der Verband zur Erhöhung der Cyberresilienz in der Schweiz bei. Dies stärkt nicht nur die Versicherungsbranche, sondern auch die gesamte Wirtschaft des Landes.

Warum erstellt der SVV einen MDR-Leitfaden?

Der SVV erstellt einen MDR-Leitfaden aufgrund seiner Schadenerfahrungen in der Versicherungsbranche. MDR-Dienste haben sich als sehr effektive Mittel zur Erhöhung der Cybersicherheit erwiesen. Viele Anbieter und Reseller in der Schweiz bieten mittlerweile ein gutes Preis-Leistungs-Verhältnis für solche Dienste an. Durch den Leitfaden möchte der SVV seinen Mitgliedern und anderen Unternehmen helfen, die besten Lösungen für ihre spezifischen Bedürfnisse zu finden. Damit wird ein wichtiger Beitrag zur Sicherheit der Schweizer Wirtschaft geleistet.