Managed Detection & Response

KUNDEN-INFORMATIONSBLATT

In collaboration with accenture

vodafone business

Prävention und Schutz vor Cyberangriffen

Einführung

Die Netzwerke sind in den letzten Jahren immer komplexer geworden. Gleichzeitig sind Cyber-Kriminelle immer raffinierter geworden und nutzen neue Methoden und zunehmend zerstörerische Waffen wie Ransomware. Im Einklang mit den Compliance-Anforderungen sollten alle Unternehmen über ein vollständiges Sicherungs- und Wiederherstellungssystem verfügen, das dazu beiträgt, die Auswirkungen eines solchen Angriffs zu verringern. Es ist ein ständiger Kampf um die Sicherheit von Netzwerken und Daten.

Es reicht nicht mehr aus, nur eine Firewall zu haben und an den Netzwerkgrenzen nach potenziellen Angreifern zu suchen. Der Analyse von Sicherheits- und Ereignisprotokollen muss mehr Aufmerksamkeit gewidmet werden. So können die Benutzer Angriffe erkennen und schnell reagieren. Den meisten Unternehmen fehlen jedoch die erforderlichen Fähigkeiten und Ressourcen, um die Analyse selbst durchzuführen.

Unser Managed Detection and Response (MDR)-Service bietet die Werkzeuge, das Fachwissen und die Ressourcen, die für die kontinuierliche Überwachung von Netzwerken und die Alarmierung bei potenziellen Bedrohungen erforderlich sind. Er ermöglicht den Kunden den Zugang zu einer Reihe von Experten, darunter Security Analysten und spezialisierte Ingenieure. Sie stehen zur Verfügung, um das Netz zu überwachen und zu verwalten, potenzielle Bedrohungen zu untersuchen und gegebenenfalls Gegenmaßnahmen zu empfehlen.

Bereitstellung des Service

Die Bereitstellung ist ein kontinuierlicher Zyklus mit vier integrierten Phasen:

- **Protokollerfassung und -transport**: MDR sammelt Security Protokolle von Client-Devices über unsere proprietäre Software Log Collection Platform (LCP). Die LCP sammelt, komprimiert und liefert Ereignisprotokolle sicher und effizient an die AWS-Umgebung von MDR zur Speicherung, Analyse und Korrelation. Die Daten werden bei der Übertragung verschlüsselt.
- **Analyse und Sicherheitsüberwachung:** Sobald die Protokolle die MDR-Plattform erreichen, konvertiert eine Data-Normalization-Engine die Protokolle automatisch in ein einheitliches, standardisiertes Format. Analyse-Engines bieten eine kontinuierliche Echtzeitanalyse von Security-Daten, die von Security Devices (Firewalls, NIDS, NIPS, HIDS, Betriebssystemen, Anwendungen usw.) erzeugt werden. Die Security-Daten werden kontinuierlich überprüft, um Instanzen und/oder Muster von potenziell bösartigen Aktivitäten zu isolieren.
- **Analyse und Reaktion auf Sicherheitsereignisse:** Auf der Grundlage zuvor festgelegter Eskalationsverfahren überprüfen Security Analysten potenziell bösartige Aktivitäten und reagieren darauf. Sobald die Analysten ihre Überprüfung abgeschlossen haben, klassifizieren sie die Security Events in vier Stufen: informational, warning, critical und emergency. Der Analyst nutzt seine Erfahrung, sein Fachwissen, die Daten, die ihm von globalen Analyse- und Nachrichtensystemen zur Verfügung gestellt werden, sowie den Kontext, den er über die Umgebung, die Anlagen und die Schwachstellen hat, um die Wahrscheinlichkeit zu bestimmen, ob diese Events negative Auswirkungen haben werden oder sich bereits negativ ausgewirkt haben.
- **Darstellung von Sicherheitsereignissen:** Alle Security Incidents, die an den Kunden eskaliert wurden, werden auf unserem Managed Detection and Response (MDR)-Portal zur Überprüfung bereitgestellt. Dazu gehören Übersichtsseiten, Informationen über kritische neue Bedrohungen, Schwachstellen und Empfehlungen zu MDR-Aktivitäten als Reaktion auf Security Incidents und Bedrohungen für das Netzwerk unserer Kunden. Kunden

können auch eine Organisationshierarchie (OH) einrichten, um verschiedene interne Funktionen und Eskalationspfade zu trennen, die eine Rollentrennung und Berichterstattung bei gleichzeitiger Transparenz im gesamten Unternehmen ermöglichen.

Vorteile

- **Umfassende Sichtbarkeit:** MDR konzentriert sich auf die gesamte Angriffsfläche, damit bekannte und unbekannte Bedrohungen erkannt und beseitigt werden können.
- **Schnelle Identifizierung und Behebung von Incidents:** Die Komponenten des MDR sind so konzipiert, dass sie eine Umgebung kontinuierlich überwachen, um anomale und bösartige Aktivitäten zu erkennen. Dies ermöglicht eine frühzeitige Erkennung potenzieller Bedrohungen in kürzester Zeit.
- **Expertenwissen:** Experten für Cybersicherheit sind teuer und schwer zu finden. Der MDR-Service ermöglicht es den Kunden, sich auf das zu konzentrieren, was für ihr Unternehmen am wichtigsten ist, und mehr zu investieren, während sie die hochspezialisierten Cybersicherheitsaktivitäten einem vertrauenswürdigen Team von Fachleuten überlassen.
- **Schnelle Identifizierung und Behebung von Incidents**: Die Komponenten des MDR sind so konzipiert, dass sie eine Umgebung kontinuierlich überwachen, um anomale und bösartige Aktivitäten zu erkennen.
- **Bemerkenswerte Kundenerfahrung**: Wir bieten unseren Kunden einen Service, der Einfachheit und operative Exzellenz bietet. Expertenwissen: Experten für Cybersicherheit sind teuer und schwer zu finden. Wir sind auch stolz darauf, dass wir unseren Kunden die Möglichkeit geben, direkt mit den Fachleuten in Kontakt zu treten.
- **Einfache Preisgestaltung**: Wir vereinfachen die Preisgestaltung von MDR, indem wir die Kosten pro Knoten und nicht pro Ereignis pro Sekunde (EPS) berechnen. Bemerkenswerte Kundenerfahrung: Wir bieten unseren Kunden einen Service, der Einfachheit und operative Exzellenz bietet.
- **Optimierte Investitionen**: Wir können vorhandene Tools und Technologien nutzen, um auf integrierte und konsolidierte Weise mehr Wert und Erkenntnisse zu gewinnen.
- **Oberfläche, auf die es ankommt**: Wir vereinen unvergleichliche globale Bedrohungsdaten, eine Plattform, die von mehreren Analyse-Engines angetrieben wird, und hochqualifizierte Cyber-Krieger, um das Rauschen zu filtern und dem Kunden zu helfen, fundierte Entscheidungen zu treffen, um die Risiken für sein Unternehmen zu mindern.

Use Cases

- Unternehmen geraten zunehmend ins Visier von Ransomware, und Cyberkriminelle beginnen damit, ihre Opfer beim Namen zu nennen, was die Rufschädigung noch verstärkt.
- Viele Unternehmen führen nur die minimalen Sicherheitsmaßnahmen durch, die erforderlich sind, um die Vorschriften einzuhalten - was den Cyberkriminellen das Leben leichter macht und die Unternehmen anfälliger für Angriffe werden lässt.
- Eine gute Sicherheitsstrategie kann Angriffe erkennen, wenn sie geschehen - eine wirklich wirksame Strategie kann jedoch Angriffe verhindern.
- Wenn ein Unternehmen seine Vermögenswerte, seine Prozesse und seine Schwachstellen genau kennt, kann es mit Hilfe von MDR Angriffe erkennen und verhindern.
- Eine wirksame Cyber-Resilienz-Strategie erfordert ein gutes Verständnis der potenziellen Bedrohungsakteure - und des menschlichen Faktors, der bei vielen Angriffen eine wesentliche Rolle spielt.
- Auch Altsysteme, auf denen neue Anwendungen installiert werden, sind anfällig für Angriffe.

vodafone business

In collaboration with

accenture