Hacker-Jagd statt Post-Mortem-Forensik

secion bietet Active Cyber Defense als 24/7 Managed Service

Hamburg, 19. November 2020 – Durchschnittlich vergehen mehr als sechs Monate, bis eine Kompromittierung durch Cyberkriminelle im Netzwerk erkannt wird.[1] Für eine drastische Verkürzung dieser Zeitspanne sorgt ab sofort der Active Cyber Defense (ACD)-Service der secion GmbH, IT-Sicherheitsspezialist und IT Security Division der Unternehmensgruppe Allgeier. Auf Basis von Threat Hunting- und Incident Response-Mechanismen werden Netzwerke 24/7 proaktiv und kontinuierlich auf Anomalien analysiert und so die Kommunikation der Angreifer zu den Command & Control-Servern (C&Cs) identifiziert.

Nahezu wöchentlich wird von spektakulären Cyberangriffen berichtet. Auch bedeutende marktführende Unternehmen sind immer wieder betroffen. Es ist offensichtlich, dass diese Angriffe trotz erheblicher IT Security-Budgets und etablierter Sicherheitslösungen, wie Antivirus, Endpoint Protection, Firewalling und IDS/IPS, in zunehmendem Maße erfolgreich sind. Damit zeigt sich, dass diese Schutzmaßnahmen für aktuelle Bedrohungen nicht mehr ausreichend sind – und für Angreifer lediglich ein Ärgernis, jedoch kein tatsächliches Hindernis darstellen.
Die secion IT-Sicherheitsexperten sehen als Konsequenz einen bedeutenden Paradigmenwechsel in der IT Security: Der Bereich Prävention ist lediglich als Teilbereich einer IT-Sicherheitsstrategie zu sehen.
„Entscheidend für die Netzwerksicherheit von Unternehmen ist es, frühzeitig in das Netzwerk eingedrungene Angreifer zu identifizieren“, sagt Marcus Henschel, Geschäftsführer der secion GmbH. „Mit unserem Active Cyber Defense-Service werden Angriffsaktivitäten im Netzwerk umgehend sichtbar gemacht. Unsere Kunden sind damit gemeinsam mit uns in der Lage, die Reaktion auf einen Sicherheitsvorfall von Monaten auf wenige Tage oder sogar Stunden zu verringern – und so den Vorsprung von Cyberkriminellen erheblich zu verringern.“

ACD als Bindeglied zwischen Protection und Response

Der ACD-Service identifiziert frühzeitig mögliche Kompromittierungen und unterstützt somit als weiterer Security Layer den Protection- und Response-Prozess proaktiv. ACD unterscheidet sich wesentlich von klassischen Maßnahmen des Bedrohungsmanagements wie Firewalls, Intrusion Detection Systems (IDS) und Sandboxing. Die Funktionsweise des Service basiert auf der Annahme, dass sich der Angreifer bereits unbemerkt Zugang zum Unternehmensnetzwerk verschafft hat. Indem

[1] *Ponemon Insitute, 2018 IBM Global Breach Study

verdeckte Indicators of Compromise (IOCs) ausfindig gemacht werden, lassen sich erfolgreiche Angriffe erkennen.
Es wird so eine Identifizierung von Sicherheitsvorfällen unmittelbar nach erfolgter Kompromittierung eines Systems erreicht – und nicht erst nach der riskanten durchschnittlichen Zeitspanne von sechs Monaten, in denen sich Angreifer unbeobachtet im Netz bewegen, weiter ausbreiten und beliebig Daten ausleiten oder manipulieren.
Mit Active Cyber Defense werden darüber hinaus Regelverletzungen, nicht gepatchte Systeme, riskantes Benutzerverhalten und möglicherweise unbekannte Angriffsflächen in der Netzwerkumgebung identifiziert.

Die Key Features von Active Cyber Defense auf einen Blick:

- **Überwachung aller Netzwerksysteme**, z.B. Desktops, Laptops, Mobiltelefone, Tablets, Server, Netzwerkgeräte, Drucker, IoT, ICS sowie BYOD.
- Nutzung erfordert **keine Installation von Agents auf Clients** – es wird auf Netzwerkebene geprüft, ob Systeme zu Command & Control-Servern kommunizieren und somit potenziell kompromittiert sind.
- Durch **Erkennen von auffälligem Kommunikationsverhalten** identifiziert ACD kompromittierte Systeme.
  Hierdurch können diese gezielt isoliert und zügig bereinigt werden.
- Wird ein aktiv laufender Angriff identifiziert, stehen dem auftraggebendem Unternehmen bei Bedarf sie secion IR-Experten unmittelbar zur Seite.
- Die secion **IR-Prozesse sind speziell auf ACD abgestimmt:** Kunden erhalten von direkt ein umfassendes Lagebild und werden von dem Expertenteam bei der Implementierung effektiver Gegenmaßnahmen begleitet.

ACD wird von secion als 24/7 Managed Service zu einem monatlichen Lizenzpreis von 1.300 EUR* angeboten. Weitere Informationen finden Sie unter *https://www.secion.de/active-cyber-defense-service*.

* Monatlicher Lizenzpreis/Mirror Port, zzgl. Set-up Fee von 1.600 EUR

Marcus Henschel, Geschäftsführer
der secion GmbH, Allgeier Company

Über die secion GmbH

Gegründet im Jahr 2004, hat sich die secion GmbH als führender Spezialist für IT-Sicherheit in Deutschland etabliert. Das Unternehmen mit Sitz in Hamburg ist als IT-Security Division Teil der international agierenden Unternehmensgruppe Allgeier. Das Leistungsspektrum von secion umfasst die Bereiche Cyber Strategy, Cyber Resilience und Cyber Defense. Mit Penetrationstests, Cyber Security Workshops sowie Lösungen im Bereich Cybererkennung und -abwehr gewährleisten die secion-Consultants die 24/7-IT-Sicherheit für vernetzte Informationsinfrastrukturen – und erreichen damit ein Höchstmaß an Unternehmenssicherheit für ihre Kunden.
Um ihre Erfahrungen mit den deutschen Unternehmen zu teilen, ist die secion GmbH Partner der Allianz für Cyber-Sicherheit, einer Initiative des Bundesamts für Sicherheit in der Informationstechnik (BSI). Weiterführende Informationen unter www.secion.de.

Weitere Informationen:

secion GmbH
Paul-Dessau-Str. 8
D-22761 Hamburg
Telefon: 040/38 90 71-0
Fax: 040/38 90 71-299
www.secion.de

Ansprechpartnerin:
Svenja Koch
Senior Marketing Managerin
Tel.: 040/38 90 71-124
E-Mail: sk@secion.de

Kommunikationsagentur:
Sprengel & Partner GmbH
Nisterstraße 3
D-56472 Nisterau
www.sprengel-pr.com

Ansprechpartnerin:
Samira Liebscher
Marketing Consultant
Tel.: +49 (0)26/61-91 26 0-0
E-Mail: sl@sprengel-pr.com