AKAMAI-KUNDENREFERENZ

Unternehmen zur Bekämpfung von Datendiebstahl nutzt Akamai zur Reaktion und Wiederherstellung bei Ransomware-Angriffen

Umfassende Netzwerktransparenz

Übergreifende Segmentierung von IT-Infrastrukturen

Reaktion auf Ransomware-Bedrohungen

Der Kunde

Ein globaler Maschinenhersteller hat nach einem großen Sicherheitsvorfall ein US-amerikanisches Unternehmen zur Bekämpfung von Datendiebstahl engagiert.

Die Herausforderung

Sich schnell ausbreitende Ransomware

Nach einem erfolgreichen Malware-Angriff, der sich schnell ausbreitete und sich auf den Geschäftsbetrieb auswirkte, kontaktierte der globale Hersteller das Unternehmen zur Bekämpfung von Datendiebstahl, um die Sicherheit in seiner Umgebung wiederherzustellen und zu verbessern. Der Angriff, der vom Laptop eines Mitarbeiters ausgelöst wurde, hatte sich schnell ausgebreitet und betraf die meisten Betriebsstandorte sowie die Backup-Server des Unternehmens.

Auswahl der richtigen Lösung

Die ersten Eindämmungsversuche, wie die Anwendung von Richtlinien zur Beschränkung des Internetzugangs über Firewalls, konnten den sich schnell ausweitenden Angriff kaum aufhalten. Aufgrund der komplexen Umgebung und der Vernetzung in einem verteilten Unternehmen erwies sich die Implementierung und Durchsetzung von Beschränkungsregeln mit Firewalls als langsam und ineffektiv.

Darüber hinaus hatte das Vorfallteam, das für die Untersuchung und Eindämmung des Angriffs verantwortlich war, erhebliche Probleme, Einblicke in die älteren Maschinen zu erhalten. Angesichts der dringlichen Lage und der Notwendigkeit, die Segmentierung zu beschleunigen, bevor der Angriff sich durch laterale Bewegung auf weitere Ressourcen ausbreiten konnte, empfahl das Unternehmen zur Bekämpfung von Datendiebstahl Akamai Guardicore Segmentation.

Unternehmen zur Bekämpfung von Datendiebstahl

Branche
Informationstechnologie

Lösung
Akamai Guardicore Segmentation

Die wichtigsten Vorteile

- Verringert die Ausbreitung von Ransomware durch laterale Netzwerkbewegung
- Bietet detaillierte Transparenz der Netzwerkvorgänge
- Schützt moderne und ältere Maschinen
- Ermöglicht eine schnelle Reaktion auf Vorfälle

Akamai

Vorteile von Akamai Guardicore Segmentation

Sofortige Sichtbarkeit

Innerhalb von nur drei Stunden stellte das Unternehmen zur Bekämpfung von Datendiebstahl Akamai-Agents auf mehr als 3.000 Unternehmensservern bereit. Und nur wenige Minuten nach der Implementierung standen detaillierte Einblicke in das Netzwerk und die Kommunikation zur Verfügung, sodass das Vorfallsreaktionsteam den Kontext und die genauen Daten erhielt, die es zur Untersuchung des Angriffs und Validierung der Eindämmung benötigte.

Schnelle Einführung von Richtlinien

Kurz nachdem sie die dringend benötigten Einblicke erhalten hatten, ergriffen die Teams Maßnahmen, um kritische Ressourcen aus der gesamten Umgebung zu segmentieren. Zwei unverzichtbare Produktionsanwendungen, die für die einzige funktionierende Fertigungslinie verantwortlich waren, wurden schnell identifiziert und gesichert. Mithilfe von Akamai Guardicore Segmentation wurde sofort eine Richtlinie zur Einschränkung von Verbindungen infizierter Subnetze und Teile des Rechenzentrums zu den Anwendungen etabliert – eine Aufgabe, die mit älteren Firewalls Wochen gedauert hätte.

Eine einfache Abfrage ergab auch, dass ältere Maschinen, die mit dem Internet verbunden waren, alte Firewalls umgehen und versuchten die Eindämmungsbeschränkungen umzusetzen. Nach der Entdeckung einer nicht konformem Kommunikation erstellte das Team Richtlinien, die den Internetzugang für alle Server, einschließlich der älteren Maschinen, innerhalb weniger Minuten effektiv einschränkten.

Laterale Netzwerkbewegung während der Wiederherstellung verhindern

Im nächsten Teil des Wiederherstellungsprozesses hat das Team die Anwendungscluster des Herstellers neu erstellt und Akamai-Agents darin eingebunden. Sie haben eine erste Richtlinie konfiguriert, die alle eingehenden Verbindungen blockiert hat, und Akamai Guardicore Segmentation verwendet, um Abhängigkeiten zu identifizieren. Anschließend wurde nur die nötigste Kommunikation zugelassen, und das auch erst nach einer Überprüfung der Anforderungen und einer Identifizierung des Kontexts. Mit diesem Ansatz konnte das Team die von dem Ransomware-Angriff betroffenen Anwendungen wiederherstellen und ohne das Risiko einer erneuten Infektion wieder online bringen.

Zukünftiger Schutz

Akamai Guardicore Segmentation ermöglichte es dem Unternehmen zur Bekämpfung von Datendiebstahl, einen erheblichen Mehrwert für seinen Kunden, den Hersteller, zu bieten und ihn bei der Wiederherstellung nach dem Ransomware-Angriff zu unterstützen. Dadurch konnte das Dienstleistungsunternehmen seinen Umsatz steigern, seine Präsenz ausbauen und Kunden dabei unterstützen, ihre IT- und Sicherheitsziele besser zu erreichen.

Durch die während der phasenweisen Wiederherstellung eingeführte interne Segmentierung des Rechenzentrums wurde die Angriffsfläche erheblich reduziert. Heute hat sich die Sicherheitslage des Unternehmens verbessert, und zukünftige Sicherheitsverstöße werden erheblich weniger Auswirkungen haben.

Weitere Informationen finden Sie unter akamai.com/guardicore.

> Mit [Akamai] konnten wir innerhalb von vier Stunden verhindern, dass der Angriff sich ausbreitete, und die ausgefallenen Produktionslinien in einem ‚sterilen' Netzwerksegment wiederherstellen, ohne das zugrunde liegende Netzwerk modifizieren zu müssen. Gleichzeitig fanden laufende IR-Untersuchungen und Eindämmungen statt.
>
> CISO beim Unternehmen zur Bekämpfung von Datendiebstahl

 | Support | Veröffentlicht: 06/23