

06. März 2024

Zusammenfassung des Vorfalls

Ein Netzwerkausfall am 6MAR2024 beeinträchtigte den Zugriff über das Frontend auf das Cyber Crucible Dashboard sowie den Telemetriezugriff über die API. Dieses Problem wurde inzwischen am 7MAR2024 behoben.

Ursache

Um 0400 UTC am 6MAR2024 begann der Telemetrieverkehr eskalierend anzusteigen und erreichte schließlich 1600 % des normalen Agenten-Datenverkehrs. Zusätzlich begann sich die Netzwerkbandbreite zwischen den AWS-Instanzen auf begrenzte Geschwindigkeiten zwischen den AWS-gehosteten Load Balancern, Servern und Datenbanken zu drosseln. In mehreren Zonen waren die Bandbreitenbeschränkungen unterschiedlich stark ausgeprägt und reichten von vollständigem Übertragungsverlust (0 % der Kapazität) bis zu 50 % der Kapazität. Auch die Verfügbarkeit des AWS-DNS war beeinträchtigt. Es wurde bestätigt, dass der eingehende Netzwerkverkehr zu Cyber Crucible gültiger Agenten-Datenverkehr bestehender Kunden war. Der Bot-Datenverkehr zu den Load Balancern nahm im Volumen nicht zu. Die zusätzliche Bandbreite war nicht die Hauptursache für die Nichtverfügbarkeit der Server, verschärfte jedoch die Bandbreitenprobleme bei Middleware und Datenbank. Der Anstieg des Agenten-Datenverkehrs in diesem Zeitraum hat sich teilweise wieder gelegt. Zum aktuellen Zeitpunkt kommuniziert Cyber Crucible keinen Zusammenhang zwischen den am 6MAR2024 gemeldeten Cloud-Ausfällen und den AWS-Problemen bzw. dem Anstieg des Datenverkehrs.

Auswirkung

Der Zugriff auf das Cyber Crucible Dashboard und die APIs wäre verzögert oder nicht verfügbar gewesen.

Die Telemetrie von installierten Agenten blieb vollständig erhalten und konnte bei der Übermittlung an die Datenbank verzögert sein, es ging jedoch keine Telemetrie verloren. Die Endpunktschutzfunktionen der Agenten waren vollständig unbeeinträchtigt und funktionierten normal, da keine Analyse- oder Schutzfunktionen von einer Netzwerkverbindung zu vorgelagerten APIs abhängen. Zum aktuellen Zeitpunkt hat die gesamte Telemetrie im Dashboard „aufgeholt“.

Behebung

Cyber Crucible hat mehrere Server sowohl innerhalb als auch außerhalb von AWS eingerichtet. Die Netzwerkstabilität innerhalb von AWS scheint sich über Nacht (7MAR2024) verbessert zu haben, wobei bereits ab 0200 UTC Verbesserungen beobachtet wurden. Cyber Crucible arbeitet derzeit mit 500 % der Serverkapazität, berechnet auf Basis der Spitzenbandbreite des Datenverkehrs, die inzwischen zurückgegangen ist. Das Team hat AWS-gehostete Server ersetzt, sobald diese die Netzwerkverbindung verloren.

Um es klar zu sagen: Eine zusätzliche Serverskalierung war in diesem Fall keine wirksame Lösung. Cyber Crucible hat begonnen, sich von AWS als alleinigem Cloud-Hosting-Anbieter zu lösen. Arbeiten zur Unterstützung einer Cloud-Plattform-unabhängigen Architektur laufen bereits seit Monaten, mit ursprünglichen Plänen, sich im zweiten Quartal 2024 von AWS als alleinigem Anbieter zu lösen. End-to-End-Tests, einschließlich aller

erforderlichen Doppelverschlüsselungs- und x509-Authentifizierungsschemata für unsere verschiedenen Server und Dienste, wurden Ende Februar 2024 abgeschlossen. Die Netzwerkprobleme, die wir mit AWS erlebt haben, haben die ursprünglich für Q2 geplante Umstellung beschleunigt, sodass sie nun einen Monat früher als

geplant beginnt.

Revision #1

Created 2026-07-24 04:22:44 UTC by Dennis Underwood

Updated 2026-07-24 04:22:44 UTC by Dennis Underwood