kyndryl

Geopolitical Tension Checklist (GTC)

Geopolitical Tension Checklist (GTC)

Die weithin berichteten zunehmenden Spannungen in Europa bergen nicht nur die Gefahr einer physischen Konfrontation, sondern auch ein erhöhtes Cybersicherheitsrisiko. Am 11. Januar 2022 veröffentlichte die U.S. Cybersecurity and Infrastructure Agency (CISA) den Cybersecurity Advisory (CSA) AA22–011A, “Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure”, in dem Einrichtungen, insbesondere Betreiber kritischer Infrastrukturen und deren Sicherheitsanbieter, aufgefordert werden, als Reaktion auf die zunehmenden Spannungen zwischen Russland und der Ukraine und die daraus resultierende Möglichkeit von Cybergefahren eine erhöhte Alarmbereitschaft an den Tag zu legen. Die CISA empfiehlt den Betreibern kritischer Infrastrukturen und ihren Sicherheitsanbietern unter anderem, alle Systeme mit Patches zu versehen, der Behebung bekannter Sicherheitslücken Vorrang einzuräumen, Antivirensoftware zu verwenden und proaktiv nach Bedrohungen zu suchen.

Darüber hinaus haben die EU- und US-Bankenbehörden Finanzdienstleister zu einer verstärkten Reaktionsbereitschaft ermahnt und am 15. Januar 2022 veröffentlichte Microsoft einen Blog-Beitrag über “destruktive Malware”, die in Systemen mehrerer ukrainischer Regierungsbehörden und Organisationen, die eng mit der ukrainischen Regierung zusammenarbeiten, beobachtet wurde. Laut Microsoft ist die “Malware als Ransomware getarnt, würde aber, wenn sie vom Angreifer aktiviert wird, das infizierte Computersystem funktionsunfähig machen.”

In Anbetracht der obigen Ausführungen empfiehlt Kyndryl seinen Kunden, so weit wie möglich alle unten aufgeführten Maßnahmen zu ergreifen. Zwar sollten auch längerfristige Maßnahmen in Betracht gezogen und umgesetzt werden, wenn sich die Situation weiterentwickelt und Regierungsbehörden und Regulierungsbehörden aktualisierte Leitlinien herausgeben, doch sollten die unten aufgeführten Maßnahmen so schnell wie möglich ergriffen werden, sobald dies möglich ist.

Empfohlene **Best-Practice-Maßnahmen**

Antizipieren - Soweit möglich, sollten die folgenden Maßnahmen zur Suche nach Bedrohungen und zur Erkennung von Anomalien die verfügbaren Daten der letzten drei bis sechs Monate analysieren:

Einleitung von **Bedrohungssuchen** zur Überprüfung der Umgebung anhand der Liste der Taktiken, Techniken und Verfahren (TTPs), die bekanntermaßen derzeit von russischen staatlich unterstützten Akteuren verwendet und ausgenutzt werden, gemäß der Warnung der US Cybersecurity & Infrastructure Agency (CISA).

Suchen Sie ungewöhnliche Login-Aktivitäten:

- Suchen Sie nach “unmöglichen Reisen”. “Unmögliches Reisen” liegt vor, wenn sich ein Benutzer relativ zeitnah von mehreren IP-Adressen aus anmeldet, die geografisch weit voneinander entfernt sind (z. B. aus zwei verschiedenen Ländern). Hinweis: Es besteht die Möglichkeit von Fehlalarmen.
- Achten Sie auf “ungewöhnliche Anmeldungen”. Zum Beispiel Logins aus Ländern, in denen Mitarbeiter, die Kunden unterstützen, nicht ansässig sind oder in denen der Kunde keine Ressourcen hat oder Geschäfte tätigt.
- Achten Sie auf eine IP, die für mehrere Konten verwendet wird, ausgenommen erwartete Anmeldungen.
- Suchen Sie nach verdächtiger Nutzung von privilegierten Konten nach dem Zurücksetzen von Passwörtern oder der Anwendung von Benutzerkontominderungen.
- Achten Sie auf ungewöhnliche Aktivitäten bei Superuser-Konten (Domänenadministrator usw.) und typischerweise ruhenden Konten.

Untersuchen Sie Ihre Kundenumgebung auf anomales Verhalten:

- Soweit verfügbar, Überprüfung von Anti-Virus- und Endpoint Detection and Response-Tools und -Daten, um ungewöhnliche Aktivitäten zu identifizieren, z. B. mehrere Systeme, die nicht reagieren, vermehrtes Auftreten von Malware/Trojanern/Viren (über das normale Maß hinaus), usw.
- Überprüfen Sie, soweit verfügbar, die Protokolle/Alarme in Ihrem Security Information Event Management (SIEM) und anderen Tools wie Firewalls, um ungewöhnliches Verhalten festzustellen (z. B. Zugriffsversuche aus neuen Ländern usw., unerwartete Daten, die die Kundenumgebung verlassen, usw.).

Schützen Sie:

- Die Infrastruktur, die für die Wiederherstellung im Falle eines Cyber-Ereignisses/ Datenverlustes benötigt wird, soweit dies möglich ist.

- Backup-/ Wiederherstellungsserver - Stellen Sie sicher, dass es brauchbare Backups der relevanten Server UND aller zugehörigen Kataloge usw. gibt. Wenn möglich - speichern Sie solche Backups in einer Offline-Umgebung, um sie weiter zu schützen. Denken Sie daran, dass die von Microsoft beobachtete Malware zerstörerisch ist - daher müssen die Backup-Server unbedingt angemessen geschützt und isoliert werden.

- Wenn Active Directory verwendet wird, implementieren Sie eine geeignete Lösung, um sicherzustellen, dass eine funktionsfähige Kopie des Active Directory verwendet werden kann, falls dies zur Wiederherstellung von Geschäftsdiensten erforderlich ist.

- Wenn DNS verwendet wird, implementieren Sie eine geeignete Lösung, um sicherzustellen, dass eine funktionsfähige Kopie des DNS verwendet werden kann, falls dies für die Wiederherstellung von Unternehmensdiensten erforderlich ist.

- Analysieren Sie, soweit möglich, die verfügbaren Backups und stellen Sie sicher, dass sie ordnungsgemäß funktionieren. Überprüfen Sie alle Rückgabecodes für Backup-Aufträge. Es werden vollständige Backups benötigt oder die Möglichkeit, einen Server und alle zugehörigen Daten neu zu erstellen.

- Überprüfen Sie das gesamte Inventar und stellen Sie sicher, dass die neuesten Patches für alle anwendbaren Schwachstellen installiert worden sind. Besondere Aufmerksamkeit ist für diese Kategorien erforderlich.

A. Mit dem Internet verbundene Systeme

B. Fernzugriff

C. Microsoft Exchange

© Copyright Kyndryl Inc. 2022. Alle Rechte vorbehalten.

Dieses Dokument ist zum Zeitpunkt seiner erstmaligen Veröffentlichung aktuell und kann von Kyndryl jederzeit ohne Vorankündigung geändert werden. Nicht alle Angebote sind in allen Ländern erhältlich, in denen Kyndryl aktiv ist. Die Garantie für die Produkte und Dienstleistungen von Kyndryl richtet sich nach den Geschäftsbedingungen der Verträge, in deren Rahmen sie bereitgestellt werden.

Die angegebenen Leistungsdaten und Kundenbeispiele dienen einzig und allein der Veranschaulichung. Tatsächliche Leistungsergebnisse können je nach spezifischen Einstellungen und Betriebsbedingungen davon abweichen. Die Garantie für die Produkte und Dienstleistungen von Kyndryl richtet sich nach den Geschäftsbedingungen der Verträge, in deren Rahmen sie bereitgestellt werden.