Gründe für eine technische Geheimhaltungsvereinbarung zur Fehlerbehebung

Inhalt

Einleitung

In diesem Dokument wird beschrieben, wann und warum eine technische Geheimhaltungsvereinbarung (NDA) für die kontinuierliche Fehlerbehebung von Cisco SWA, ESA und SMA erforderlich ist.

Produktübersicht

Bevor wir uns den Feinheiten der Tech NDA zuwenden, werden wir uns zunächst mit den drei genannten Produkten von Cisco vertraut machen.

- ESA (E-Mail Security Appliance).
- SWA (Secure Web Appliance), vormals Web Secure Appliance (WSA).
- SMA (Security Management Appliance)

Was ist eine technische Geheimhaltungsvereinbarung?

Eine technische Geheimhaltungsvereinbarung ist ein rechtsverbindliches Dokument, das von Cisco und Ihrem Unternehmen unterzeichnet wurde, um die Vertraulichkeit der Daten zu gewährleisten.

Dieses Dokument ist für beide Parteien rechtlich bindend und schützt sie vor der Offenlegung vertraulicher Informationen, die bei jeder Interaktion zwischen ihnen weitergegeben werden.

Wann müssen Sie eine technische Geheimhaltungsvereinbarung

unterzeichnen?

Bestimmte Produkte von Cisco bieten Kunden die Möglichkeit, einen sicheren Remote-Zugriff zu ermöglichen, sodass zulässige Cisco Techniker ihre Fehlerbehebungsfunktionen erweitern können, indem sie eine direkte Verbindung mit der Root-Shell herstellen. Wenn Sie aufgrund von Netzwerkeinschränkungen oder anderen Unternehmensrichtlinien keinen Remote-Zugriff auf die Geräte aktivieren können, ermöglicht die technische Geheimhaltungsvereinbarung Cisco, mit Ihnen zusammenzuarbeiten und auf die Root-Shell zuzugreifen, während Sie über WebEx verbunden sind, sodass Sie alle auf Ihrem Gerät ausgeführten Befehle oder Änderungen in Echtzeit überwachen können.

Dieser Zugriff ermöglicht es Technikern, Befehle auszuführen, Verzeichnisse und Protokolle zu durchsuchen, Prozesse zu überprüfen und andere Aufgaben auszuführen, die vom Front-End (dem Kunden zugewandten Bereich) des Geräts aus nicht möglich sind.

Hier einige Beispiele für mögliche Optionen für diesen Zugriff:

- Analyse von Core Dump-Dateien.
- Transparenz von Verzeichnissen und Protokollen, auf die sonst nicht zugegriffen werden kann
- Weitere Details zu Prozessen und Ressourcenverbrauch.
- Hardwarediagnose.
- Änderungen am Code.
- und mehr.

Warum müssen Sie eine technische Geheimhaltungsvereinbarung unterzeichnen?

Die Informationen aus dem Backend der Cisco Produkte werden als streng vertraulich eingestuft. Die technische Geheimhaltungsvereinbarung trägt dazu bei, sicherzustellen, dass firmeneigene Informationen von Cisco, die während eines WebEx Meetings oder zu einem anderen Zeitpunkt ermittelt wurden, nicht an Dritte außerhalb der beabsichtigten Zielgruppe weitergegeben werden.

Wie kann man eine technische Geheimhaltungsvereinbarung unterzeichnen?

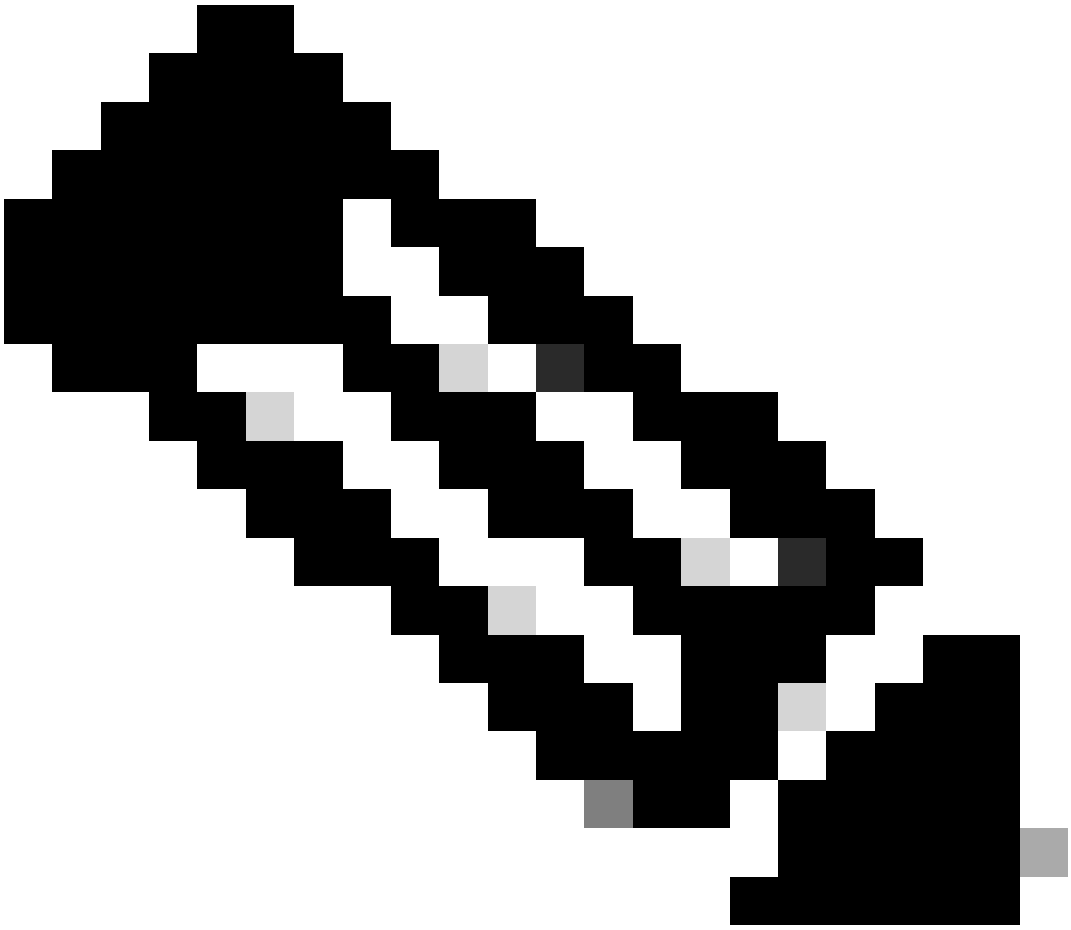
Es gibt zwei Methoden, eine technische Geheimhaltungsvereinbarung zu verwenden.

[1] Wenden Sie sich an den TAC-Techniker, der Ihrer Serviceanfrage zugewiesen ist, und senden Sie Ihnen den Entwurf der Geheimhaltungsvereinbarung per E-Mail. Unterzeichnen Sie die Bedingungen, und stimmen Sie ihnen zu. und geben Sie sie an Cisco weiter. warten Sie auf die letzte Bestätigung.

[2] Sie können Ihren Account Manager (AM) kontaktieren und folgende Informationen angeben:

- Rechtlicher Name Ihres Unternehmens
- Land
- Straße
- Stadt
- Postleitzahl
- Name der unterzeichnenden Person
- E-Mail der Person, die unterzeichnet - Dies muss aus der Domäne des Unternehmens sein

---



Hinweis: Wenn im vergangenen Jahr eine Geheimhaltungsvereinbarung für einen anderen Service Request (SR) unterzeichnet wurde, bleibt sie gültig. Geben Sie die Serviceticketnummer, die mit dieser Geheimhaltungsvereinbarung verknüpft ist, dem Eigentümer des aktuellen Tickets an.

Wer muss eine technische Geheimhaltungsvereinbarung unterzeichnen?

Eine Person, die befugt ist, das Unternehmen gesetzlich zu vertreten.

In der Regel die Person, die von Ihrem Ende an der WebEx Sitzung teilnimmt, es wird jedoch eine Person auf der Manager-Ebene empfohlen.

Zugehörige Informationen

- Technischer Hinweis zu den häufig gestellten Fragen zum Remote-Zugriff auf Cisco ESA/WSA/SMA

Informationen zu dieser Übersetzung

Cisco hat dieses Dokument maschinell übersetzen und von einem menschlichen Übersetzer editieren und korrigieren lassen, um unseren Benutzern auf der ganzen Welt Support-Inhalte in ihrer eigenen Sprache zu bieten. Bitte beachten Sie, dass selbst die beste maschinelle Übersetzung nicht so genau ist wie eine von einem professionellen Übersetzer angefertigte. Cisco Systems, Inc. übernimmt keine Haftung für die Richtigkeit dieser Übersetzungen und empfiehlt, immer das englische Originaldokument (siehe bereitgestellter Link) heranzuziehen.