在刪除附件後配置ESA防病毒掃描

目錄

簡介

本檔案介紹在思科電子郵件安全裝置(ESA)上移除附件後，是否仍需要進行防病毒掃描。

背景資訊

即使啟用了附件刪除規則，思科郵件安全裝置(ESA)也必須保持啟用防病毒掃描，因為附件刪除不能可靠地從每個郵件結構中移除所有惡意內容。

問題陳述

管理員可以假定刪除附件會消除惡意軟體風險，並且無需進行防病毒掃描。本文說明為什麼在移除附件後仍必須使用防病毒掃描。

環境

本指南適用於思科電子郵件安全裝置(ESA)處理的入站和出站電子郵件。

建議

即使思科郵件安全裝置(ESA)上啟用了附件刪除規則，郵件也需要防病毒掃描。

配置附件刪除策略後，對所有適用的郵件流啟用防病毒掃描。

- 掃描入站電子郵件，因為惡意內容可能保留在附件刪除規則未刪除的郵件部分中。
- 掃描出站電子郵件，因為在附件刪除處理後，郵件仍可能包含惡意軟體。
- 期望通過刪除附件規則來降低風險，而不是取代防病毒掃描。

附註：預期結果：刪除附件可以減少一些基於檔案的威脅的暴露情況，但是仍需要防病毒掃描來檢測郵件中保留的惡意內容。範圍：本指南說明刪除附件後是否仍需要防病毒掃描；它不會描述ESA上的所有惡意軟體檢測功能。

為什麼刪除附件是不夠的

刪除附件可以減少風險，但不能消除風險。

- 附件不是一個嚴格的技術定義。
- ESA評估RFC定義的MIME部分，而不是通用附件對象。
- 報文可以繞過附件丟棄邏輯的方式構造，因為術語「附件」不是一個精確的技術定義。
- 由於電子郵件內容可以採用不同的MIME格式構建，因此附件刪除規則無法可靠地刪除所有惡意內容。
- 出站郵件仍然可以攜帶惡意軟體。

相關資訊

有關詳情，請參閱：

- ESA消息過濾器操作說明
- 使用郵件過濾器

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。