删除附件后配置ESA防病毒扫描

目录

[简介](#)

[背景信息](#)

[问题陈述](#)

[环境](#)

[建议](#)

[为什么删除附件还不够](#)

[相关信息](#)

简介

本文档介绍在删除思科邮件安全设备(ESA)上的附件后，是否仍需要进行防病毒扫描。

背景信息

即使启用了附件丢弃规则，思科邮件安全设备(ESA)也必须保持启用防病毒扫描，因为附件删除不能可靠地从每个邮件结构中移除所有恶意内容。

问题陈述

管理员可以假设删除附件可消除恶意软件风险，并且无需进行防病毒扫描。本文解释删除附件后仍必须使用防病毒扫描的原因。

环境

本指南适用于思科邮件安全设备(ESA)处理的入站和出站邮件。

建议

即使思科邮件安全设备(ESA)上启用了附件丢弃规则，邮件也需要防病毒扫描。

在配置附件删除策略后，为所有适用的邮件流启用防病毒扫描。

- 扫描入站电子邮件，因为恶意内容可能保留在附件删除规则未删除的邮件部分中。
- 扫描出站电子邮件，因为在附件删除处理后，邮件仍可能包含恶意软件。
- 期望通过删除附件规则来降低风险，而不是取代防病毒扫描。



注意：预期结果：删除附件可降低对某些基于文件的威胁的风险，但仍需进行防病毒扫描以检测邮件中保留的恶意内容。范围：本指南介绍删除附件后是否仍需要防病毒扫描；它不会描述ESA上的所有恶意软件检测功能。

为什么删除附件还不够

删除附件可以减少风险，但不能消除风险。

- 附件不是严格的技术定义。
- ESA评估RFC定义的MIME部分，而不是通用附件对象。
- 由于术语“附件”不是一个精确的技术定义，因此可以采用绕过附件丢弃逻辑的方式构建邮件。
- 由于电子邮件内容可以采用不同的MIME格式构建，附件丢弃规则无法可靠地删除所有恶意内容。
- 出站邮件仍然可以携带恶意软件。

相关信息

有关详细信息，请参阅:

- ESA邮件过滤器操作说明
- 使用邮件过滤器

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。