思科邮件安全设备(ESA)向您的组织发送垃圾邮件

目录

简介

本文档介绍垃圾邮件可以进入贵组织的五种方法。

方法

1.合法邮件/营销邮件

合法消息已由用户选择输入，或者其名称已出售给其他组织。在第一种情况下，用户需要采取步骤取消订阅列表。如果是后者，请再次将邮件提交到spam@access.ironport.com，以便反垃圾邮件定义可以全局更新，从而提高ESA的整体垃圾邮件捕获率。在“传入邮件”策略中启用“营销”邮件有助于改变此邮件“营销”而非“垃圾邮件”的感觉。

2.反垃圾邮件更新不正确

反垃圾邮件已禁用或功能密钥已过期。要检查并查看反垃圾邮件是否正在更新，请转**到GUI >安全服务> IronPort Anti-Spam。在此面板中，您应在过去6小时内看到规则集或引擎的更新。**此外，您还可以从顶部的此选项卡中确保启用反垃圾邮件服务。要查看功能密钥状态，您可以转到系统管理选项卡>功能密钥以检查反垃圾邮件密钥的状态。

3.邮件策略或邮件过滤器

如果根据客户邮件策略，针对特定发件人或收件人禁用了反垃圾邮件安全引擎，则垃圾邮件可以进入您的组织。 跳过垃圾邮件过滤的另一种方法是通过邮件过滤器(CLI:**filters**命令)。

4.邮件流策略

使用消息的ICID对消息进行分类。在这种情况下，反垃圾邮件安全功能很可能被关闭，这会覆盖邮件策略。您可以通过查看邮件日志来确定这一点，在日志中，您首先需要查看ICID，以了解邮件被归类到哪个发件人组。从此处查看关联的邮件流策略。如果您的AllowList中有大量条目，则可能需要查看一些正在进入的邮件，以查看它们是否被反垃圾邮件引擎扫描。打开邮件的报头并查找报头X-IronPort-Spam，此报头的存在意味着邮件确实通过了引擎。

5.邮件是垃圾邮件

邮件是实际垃圾邮件。您已确认反垃圾邮件引擎已使用邮件跟踪功能扫描邮件（在邮件跟踪中，查找“CASE”）。 如果判例为否定，并且您认为邮件是垃圾邮件，请将原始邮件提交到 spam@access.ironport.com。这可能是新垃圾邮件威胁刚刚发布或旧威胁重新设计的情况。

垃圾邮件提交的处理过程既是自动的，也是手动的，对于您的特定提交没有反馈。您可以随时联系思科TAC并请求评估和响应。