DELL Technologies

中间人 (MITM)：携手 Dell Technologies 加强网络安全和弹性

中间人 (MITM) 攻击的威胁不断增加

中间人 (MITM) 攻击仍然是最复杂和危险的网络安全挑战之一。此类攻击中，恶意行为者可在不被察觉的情况下拦截并篡改私人通信，各行各业不同规模的企业皆可能成为目标。从电子商务平台到金融机构，没有任何组织能够免于这种风险。MITM 攻击通常会为数据盗窃、财务欺诈和声誉损害铺平道路，在数字化转型加速的当下，这种攻击方式已成为极具破坏性的网络威胁之一。

Dell Technologies 深知企业在防范这些高级威胁时面临的独特挑战。通过提供创新且可扩展的安全解决方案，戴尔助力各类组织化解 MITM 威胁、保护资产和维护业务完整性。

中间人攻击 (MITM) 是什么?

中间人 (MITM) 攻击是指网络犯罪分子秘密拦截两方通信的行为，例如截获员工与公司服务器之间或客户与企业网站之间的数据传输。从窃取敏感数据到出于恶意目的操纵通信，攻击者的目标可能有所不同，但结果是相同的：破坏信任和安全性。

常见的 MITM 手段

攻击者使用的一些最常见的方法包括：

Wi-Fi 窃听：网络犯罪分子利用不安全或已泄露的公共 Wi-Fi 网络来拦截通信。

DNS 欺骗：攻击者通过篡改 DNS 记录将用户重定向至欺诈网站，诱骗用户无意间提交敏感信息。

会话窃取：通过窃取活跃会话凭据，攻击者会未经授权访问私人账户。

SSL 剥离：此手段会将安全 HTTPS 连接降级到易受攻击的 HTTP 连接，从而暴露敏感信息。

这种适应性使 MITM 攻击尤为险恶，因为它们往往伪装成表面看起来合法的日常业务交易和交互。

对企业的影响

MITM 攻击的连锁效应远远超出即时事件。最严重的一些后果包括：

收入损失

凭据被盗和运营干扰往往导致双重财务负担 — 既包括直接经济损失，又涉及事件恢复成本。

运营受挫

解决攻击所花费的时间和资源会影响关键业务职能，从而影响生产力和业务发展。

信任侵蚀

当客户的个人信息被泄露时，客户的信心可能会迅速瓦解，造成长期的品牌声誉损害。

监管影响

处于严格合规要求行业的企业，在数据泄露后可能面临罚款或制裁。

现实案例

一则案例为我们敲响警钟：一家全球零售企业因在线支付平台未加密，成为 SSL 剥离攻击的受害者。攻击者曾在结账环节拦截客户信用卡信息。通过快速检测机制与战略性安全措施（包括戴尔端点保护工具），该公司成功阻断攻击并减轻了长期损害。这一场景不仅揭示了中间人攻击的即时风险，更凸显出部署分层防御体系的至关重要性。

359 亿

的全球已知数据泄露量

来源：2024 年 5 月：PureWL 报告

携手 Dell Technologies，抵御 MITM 攻击

Dell Technologies 可为组织提供具有前瞻性的全面工具，旨在防范 MITM 风险，避免其造成损害。

通过戴尔可信设备，为端点提供保护

由于 MITM 威胁通常源自端点，因此端点保护成为优先事项。戴尔可信设备将先进的安全性直接嵌入到硬件中。例如：

- **Dell SafeBIOS** 可确保系统完整性得到保护，防止未经授权篡改启动顺序。
- **SafeID** 通过保护用户身份验证数据，形成防御凭据盗窃的堡垒，从而添加了一层额外保护。
- **Dell SafeData** 可提供端到端加密，保护公司防火墙内外的敏感信息，使截获的数据无法读取。

这些功能已在全球企业中部署，以加强端点系统的信任。一家跨国制造公司使用戴尔可信设备，保护其远程员工免受针对公司笔记本电脑的定向 MITM 攻击，即使在高风险差旅场景中也能确保安全连接。

通过 CrowdStrike，实现高级检测

实时检测和响应 MITM 威胁至关重要。CrowdStrike 与戴尔生态系统集成，利用人工智能和行为分析来监控和消除可疑活动。持续监控可确保混合环境（威胁往往隐匿其中）的安全防护。通过主动识别异常，企业能够在损害发生前消除潜在的 MITM 企图。

例如，一家金融机构通过高级检测技术，成功发现并阻止了面向客户的门户的入侵行为。该平台的 AI 识别出指示 SSL 剥离攻击的异常网络活动，从而实现了即时补救。

通过 Dell PowerProtect，强化数据保护

即便拥有高级防御体系的组织仍可能遭遇安全漏洞。这正是 Dell PowerProtect 的用武之地。凭借不可变性和安全隔离 Air Gap 存储等功能，可在攻击期间保护关键业务数据免受篡改、破坏或访问。PowerProtect Cyber Recovery 存储区通过将机密数据与主网络隔离，确保即使在最坏的情况下，敏感信息也保持完好且可恢复，从而提供额外的安全性。

该技术曾在一家医疗组织遭遇 DNS 欺骗攻击时发挥关键作用。通过利用 PowerProtect 的不可变备份和恢复存储区，该组织可以快速恢复运营，而不会丢失数据。

快速响应和恢复服务

戴尔的 Data Protection Services 可在发生数据泄露时提供由专家主导的快速恢复，与其现有的技术相辅相成。从远程数据恢复到事件响应，这些解决方案可减少停机时间并更大限度地减少运营中断。分秒必争之时，拥有值得信赖的合作伙伴能确保组织充满信心地恢复运营。

通过 Dell PowerSwitch Networking 和 SmartFabric OS，实现高级网络安全性和微分段

在整个基础架构中提供高级网络分段、严格的访问控制和实时流量分析，从而增强对零日攻击的防御能力。

通过多层方法，增强安全性

要全面对抗 MITM 攻击，企业必须实施多维度安全策略。Dell Technologies 重点关注以下切实可行的步骤：

- **采用零信任原则：**在每个时间点全程验证所有活动和用户访问权限，无论它们来自公司内部还是外部网络。
- **使用高级加密：**对所有通信进行端到端加密，确保截获的数据对攻击者不可用。
- **实施多因素身份验证 (MFA)：**MFA 为系统添加了多层身份验证，从而可以显著减少未经授权访问漏洞。
- **培训员工：**通过强调网络钓鱼骗局、可疑的 Wi-Fi 使用和未经验证的链接等风险，培养更警惕的员工队伍。
- **定期系统测试：**通过频繁的渗透测试和更新，识别漏洞，并确保防御措施保持最新状态。

戴尔的整体安全产品与这些实践相结合，可为不断变化的威胁提供强大且适应性强的防御措施。

战略合作伙伴关系的价值

Dell Technologies 与 CrowdStrike 和 Secureworks 等知名网络安全公司开展合作，进一步强化解决方案能力。通过这些合作伙伴关系的专业知识，戴尔能够应对各种可能的攻击载体。例如，CrowdStrike 通过利用威胁情报丰富戴尔平台来增强端点保护，而 Secureworks 可提供有关不断变化的风险的切实可行的见解，确保持续的准备和适应。

Dell Technologies Advantage

选择 Dell Technologies，意味着与网络安全创新领域值得信赖的领导者携手。无论是通过端点保护、数据恢复还是协作合作伙伴关系，戴尔的端到端解决方案都能助力组织在攻击者面前保持领先地位。

借助戴尔全面的 MITM 解决方案，保护您的业务、维护客户信任，并让您的运营未来无忧。立即联系我们，开始为您的企业打造具备弹性的安全未来。

与 Dell Technologies 合作，您可以积极应对网络威胁，与客户和利益相关者建立持久的信任，并确保在日益不安全的数字世界中取得运营成功。安全可靠的未来 — 戴尔护航，智启新程。

如需了解如何应对当今一些主要的网络安全挑战，请访问 **Dell.com/SecuritySolutions**

详细了解
戴尔解决方案

联系 Dell Technologies
专家

查看更多
资源

加入 #HashTag
对话

DELL Technologies