DELL Technologies

携手 Dell Technologies 防范供应链网络攻击

执行摘要

业务运营日益全球化和互联化的特性，使组织面临不断升级的供应链网络攻击威胁。从制造到部署以及第三方软件，这些复杂的攻击利用硬件生命周期中的漏洞，使恶意攻击者能够通过受信任的应用程序或更新危及整个系统。此类事件不仅会造成灾难性财务损失，更可能引发大规模声誉损害与运营瘫痪。

这些威胁的影响是深远的。供应链攻击往往在造成重大损害后才会被察觉，因此主动式防御策略至关重要。戴尔通过高级端点防护、主动监控以及全面的服务器和数据安全解决方案，助力企业构建端到端的供应链安全体系。依托技术优势、合作伙伴关系和专业知识，组织能够增强弹性，有效抵御其生态系统中的固有漏洞。

供应链网络攻击威胁不断上升

供应链攻击近年来大幅增加。通过在生产、运输或部署期间篡改物理设备，或者发现软件提供商的弱点，攻击者就可以获得注入恶意组件或代码、损坏系统或泄露敏感数据的手段。受害者涵盖从小型企业到跨国企业的各类组织，导致的严重后果包括：重大财务损失、客户信任体系崩塌以及法律追责风险。Dell Technologies 认识到这种日益严重的危险，并倡导采取预防性措施来减轻此类攻击的灾难性影响。

了解供应链网络攻击

硬件供应链攻击的工作原理

1. **制造阶段：**攻击者在硬件组装过程中引入恶意组件，这往往会利用受污染的供应商。
2. **运输阶段：**设备在运输过程中被拦截并遭到修改，被植入有害的固件或硬件修改。
3. **部署和激活：**被入侵的硬件进入组织的网络后，攻击者就可以访问敏感数据或启用后门操作。

软件供应链攻击的工作原理

1. **初始漏洞：**第三方软件供应商通常因网络钓鱼、未修补的漏洞或内部威胁而受到攻击。
2. **代码操纵：**恶意行为者将恶意软件或后门等有害元素注入待分发的软件中。

3. **向终端用户传播**：安装或更新受污染软件的企业无意中下载了恶意组件。

常见手段 — 硬件

- **固件操纵**：嵌入可在部署后激活的恶意代码。
- **硬件植入**：集成隐藏组件，以监控或窃取数据。
- **受信任的供应商利用**：利用安全流程较弱的第三方供应商。

常见手段 — 软件

- **组件劫持**：使用恶意代码感染第三方库或框架。
- **更新注入**：更改官方软件更新以包括漏洞。
- **依赖关系混淆**：利用组织对不安全软件包依赖关系的依赖。

对企业的影响

财务后果

针对供应链的攻击往往导致涉及法律罚款、系统恢复费用和客户赔偿。一起涉及全球 IT 管理公司的重大事件造成了超过 7000 万美元的损失，充分展现了这类数据泄露可能造成的财务破坏力。

运营中断

恶意软件渗透带来的损坏或禁用系统通常会引发大规模停机，进而破坏组织生产力并延误项目交付进度。

声誉后果

现代企业高度依赖对软件合作伙伴的信任。与组织的软件产品相关的供应链漏洞可能会损害声誉并降低客户忠诚度。

现实案例 — 硬件/软件

一家全球电子制造商发现其供应链中的组件受污染，导致大规模系统故障。此次攻击造成了超过 **4500 万美元**的恢复和法律费用，以及对供应商关系造成无法弥补的损害。

SolarWinds 安全漏洞事件堪称最臭名昭著的软件供应链攻击案例之一。其 Orion 产品的漏洞导致全球范围内的组织受到感染，波及了政府机构和《财富》500 强企业。此次事件的估计损失超过 **9000 万美元**，充分揭示了供应链漏洞可能带来的深远影响。

Dell Technologies 在应对供应链攻击方面的专业知识

Dell Technologies 广泛的安全解决方案组合可帮助企业持续领先于不断演变的网络风险。

戴尔安全组件验证 (SCV)

安全组件验证 (SCV) 是 Dell Technologies 供应链安全战略不可或缺的一部分，旨在确保各种戴尔解决方案中硬件组件的真实性和完整性。从制造到交付部署的全生命周期，SCV 可提供对系统组件的加密验证。Dell Technologies 提供强大的供应链安全保障，确保系统从出厂到部署全程防篡改且安全可靠。通过这一举措，戴尔客户将获得更全面的安全保障、更高的可靠性和更好的性能体验。

通过戴尔可信设备，为端点提供保护

戴尔可信设备在硬件和固件级别集成安全性，以创建防篡改系统。

- **SafeBIOS** 可在启动时确保固件完整性，防止未经授权的配置更改，并在启动时验证固件完整性，防止受污染的系统启动。
- **SafeID** 可在硬件级别保护身份验证凭据，阻止未经授权的访问，并通过保护身份验证密钥和锁定未经授权的用户来保护登录凭据。
- **SafeData** 支持对敏感业务文件进行端到端加密，从而有效阻断掠夺性数据窃取企图。

通过 CrowdStrike，实现主动威胁检测

CrowdStrike 与戴尔的技术相集成，可实时洞察恶意软件行为。

- **行为威胁检测分析：**监控硬件和固件行为是否有篡改迹象，并检测异常软件活动，以防止恶意软件部署。
- **即时响应工具：**AI 可隔离受污染系统，防止网络内横向移动。
- **基于 AI 的威胁补救：**主动识别和隔离威胁，防止其在企业系统内部横向扩散。
- **集成功能：**混合环境和多云环境通过戴尔和 CrowdStrike 工具得到全面保护。

通过戴尔的服务器和存储解决方案，增强安全性

Dell PowerEdge 服务器系列集成了先进的保护措施，以确保关键任务软件平台的安全。Dell PowerStore 等存储系统为应用程序和数据提供卓越的加密功能。

- **安全的服务器固件：**监控和阻止未经授权的硬件级更改。
- **隔离网络监控：**检测指示供应链篡改的异常情况。
- **不可变备份：**即使主存储受到破坏，也可保护恢复点。
- **恢复存储区：**隔离环境可防范受感染系统引发的级联故障。

降低风险的多层方法

戴尔鼓励企业采用将技术、人员实践和更新流程相结合的全面战略。

战略步骤

- **提高供应链可见性：**要求所有供应商都遵守严格的安全标准，并在每个阶段对硬件进行认证。
- **实施高级加密：**在所有级别使用高级协议保护数据，即使在受污染硬件中也能限制访问。
- **采用零信任策略：**未经验证，任何设备、应用程序或用户都不会自动获得信任。
- **安全编码标准：**与软件合作伙伴协作，强制执行有关插件、API 和集成的严格准则。
- **定期监控活动和审核：**通过频繁的可见性审核，确保第三方服务的完整性。
- **执行定期测试：**部署渗透测试和固件评估，以持续验证设备完整性。
- **培训员工：**培训团队如何识别表现出可疑行为的组件或软件包。

Dell Professional Services 如何确保业务弹性

Dell Professional Services 指导企业实施强大的供应链防御措施。一支由经验丰富的网络安全专家组成的团队，能够根据组织的独特需求提供定制化的评估、培训和威胁应对策略。

- **实施指导：**在供应商环境中，对零信任和经审计的提供商实践进行战略性调整。
- **事件响应：**确保企业在遭遇恶意事件后能够迅速恢复运营。

以戴尔为依托，打造未来无忧的企业系统

供应链网络攻击印证了现代威胁的复杂性。企业需要的保护不仅要防止漏洞，还要确保在发生事件时快速恢复。与 Dell Technologies 合作，意味着可以获得尖端工具、战略专业知识和值得信赖的协作网络。

后续行动

实施由 Dell Technologies 提供支持的最佳实践，可以保护敏感资产并简化运营可靠性。立即联系我们，获得量身定制的咨询，为保护企业系统的生命线做好充分准备。

随着供应链网络安全的发展，Dell Technologies 代表了信任、适应性和创新。今日的安全投入，铸就明日的成功基石。

安全可靠的未来 — Dell Technologies 护航，智启新程。信赖戴尔，为重要资产提供安全保障。

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