DELL Technologies

备份渗透：携手 Dell Technologies 加强网络安全和弹性

执行摘要

备份渗透专门利用为保护关键信息而设计的系统漏洞，对各个行业的企业构成了日益严重的威胁。此类攻击会破坏数据恢复系统、削弱信任并危及运营。从严重的财务损失到长时间停机和声誉损害，后果可能极为严重。

Dell Technologies 提供一整套端到端防御措施来保护敏感数据并防范此类攻击，这些措施包括戴尔可信设备、戴尔可信基础架构以及集成到我们所有解决方案中的广泛安全功能。通过建立战略合作伙伴关系及提供专业服务，戴尔助力组织构建具备弹性的多层安全框架，以高效检测、拦截备份渗透攻击并实现快速恢复。

通过实施戴尔的创新解决方案和专家支持，企业将能做好充分准备，有效保护其基础架构并保持运营连续性。

备份渗透威胁不断攀升

备份系统对于业务连续性至关重要，是应对勒索软件或硬件故障等网络事件后恢复的关键。令人遗憾的是，这些至关重要的生命线正日益成为网络犯罪分子的攻击目标。备份渗透会损坏或删除备份数据，导致其在关键时刻无法访问。

面对不断演变的威胁，必须采取主动防御措施。无法保护备份系统会危及运营并暴露敏感数据。从小型企业到跨国公司，无论规模大小，各行各业都可能成为攻击目标，特别是医疗保健、金融和制造业等行业面临的风险尤为突出。

Dell Technologies 深刻意识到强化备份环境防护的紧迫性，因此提供先进工具和指导，以应对这类复杂攻击。

备份渗透攻击

备份渗透是指网络犯罪分子利用备份系统中的漏洞破坏、删除或加密关键恢复数据。这些复杂攻击可能与勒索软件或恶意软件部署等其他事件同时发生或紧随其后，从而加剧运营和财务影响。

备份攻击的工作原理

1. **初始入侵：**攻击者通常通过网络钓鱼、弱凭据或未修补的漏洞来未经授权访问网络。
2. **横向移动：**一旦进入网络，攻击者就会利用工具隐蔽移动，锁定备份存储库和关键数据集。
3. **备份入侵：**关键手段包括加密备份文件、删除恢复点或损坏数据。

常见手段

- **凭据盗窃**会破坏管理账户，以实现对备份系统的完全访问权限。
- **勒索软件部署**会同时加密实时数据和备份，要求支付解密费用。
- **计时损坏**会逐渐影响备份以逃避检测，同时在需要恢复时让企业暴露在风险中。

这种手段突显了这些威胁的复杂性和严重性，需要采取先发制人的行动。

对企业的影响

财务损失

备份渗透会加大恢复成本和停机时间，通常会使响应费用增加两到三倍。为了从加密或受损备份中恢复，可能需要针对攻击者、新基础架构或昂贵的顾问支付费用。

运营中断

如果缺乏有效的备份，组织将面临漫长的恢复时间，这会导致服务中断、项目延迟以及关键功能停摆。

声誉后果

一旦发生永久性数据丢失或长时间停机，利益相关者对企业的信任将会削弱，这可能会影响企业的长期生存能力。

现实案例

一家全球医疗提供商在遭遇勒索软件攻击期间发现其备份已损坏。除了支付赎金，三周的患者数据永久丢失、手术延迟并引发诉讼。总恢复成本超过 **5,000 万美元。**

触目惊心的统计数据

一项最近的研究估计，如果备份系统遭到破坏，平均经济损失将超过 **445 万美元**[1]，其中包括罚款、停机时间和恢复费用。此类事件的频率不断增加，尤其令人震惊，全球报告显示，备份相关威胁同比增长 **39%。**

57%
的备份定向攻击成功渗透了备份存储库

来源：2024 年：Index Engines

携手 Dell Technologies 防范备份渗透

Dell Technologies 提供了一套强大的工具和服务，可应对备份渗透攻击带来的独特挑战，使企业能够有效地预防、检测和恢复。

服务器和存储安全解决方案

戴尔的服务器和存储解决方案可提供出色的弹性，以应对备份相关攻击。内置功能可确保备份保持安全，并且快照不会受到影响。

- **不可变备份/快照**可创建防篡改还原点。
- **安全隔离 Air Gap** 可将数据与实时网络隔离，以防止损坏。

[1] Ponemon —《Cost of a Data Breach Report 2024》

强化戴尔数据保护设备

戴尔数据保护设备内置多项防护能力，包括确保固件完整性的 Dell SafeBIOS 和实现安全加密的 SafeData，助力防范备份攻击。此外，这些解决方案还具备多因素身份验证(MFA)、基于角色的访问控制 (RBAC) 和双重身份验证等功能，可有效阻止威胁入侵者。

通过 CrowdStrike，实现高级威胁检测

CrowdStrike 与戴尔数据保护相集成，侧重于通过一组高级功能来增强数据保护环境的安全性和监控能力。

1. **端点和数据保护：**戴尔将 CrowdStrike 的端点安全性及扩展检测和响应 (EDR/XDR) 与其数据保护解决方案集成在一起。这包括来自 Dell PowerProtect Data Manager 和 PowerProtect Data Domain 的遥测数据收集，以及来自 CrowdStrike Falcon 控制台和下一代 SIEM 软件的安全洞察
2. **监控和响应：**Dell Managed Detection and Response (MDR) 服务代表客户管理 CrowdStrike 软件、收集日志并调查任何入侵指标 (IOC) 或异常检测。这种集成使戴尔能够提供持续监控并与客户的 SOC 协作，以确保快速、有效地补救威胁事件
3. **实时可见性和数据移动控制：**CrowdStrike Falcon Data Protection 平台可提供跨各种来源和渠道的数据移动的实时可见性，并按内容和上下文对数据进行分类。将内容与上下文分析相结合，有助于防止数据被盗并确保有效实施数据保护策略
4. **统一管理和简化部署：**此集成允许单一平台和代理同时管理端点和数据保护，从而降低复杂性和运营开销。这得益于 CrowdStrike Falcon 平台采用的轻量级云原生方法，可实现快速部署并更大限度地减少中断

CrowdStrike 与 Dell Data Protection 相集成，通过高级 EDR/XDR 功能、实时监控和全方位数据管理，显著提升数据保护环境的整体安全性与弹性。

一家主要金融机构在近期部署了 PowerProtect Cyber Recovery，可在数据泄露期间阻止攻击者访问 90% 的关键备份，从而实现无缝恢复，而无需支付赎金。

通过 Dell PowerProtect 解决方案，实现备份完整性

通过利用不可变性、隔离和压缩等技术，Dell PowerProtect 为备份系统提供了全面的保护，防止备份系统受到损害。通过与勒索软件检测工具集成，PowerProtect 可确保在出现可疑更改时触发警报，以便立即采取行动。

多层安全方法

数据保护需要协调统一的多层面安全策略。戴尔帮助企业实施行业最佳实践，以构建弹性备份环境。

增强防御的关键步骤

- **采用零信任原则：**持续验证所有用户、设备和流程，降低未经授权访问的风险。
- **加密所有备份：**确保数据在损坏时保持不可读状态，无论是传输中数据还是静态数据。
- **培训员工：**指导员工识别网络钓鱼企图和其他导致初始违规的社会工程手段。
- **定期漏洞测试：**通过频繁测试，帮助组织在攻击者利用漏洞之前发现漏洞并修补薄弱环节。

戴尔将这些实践与尖端解决方案相结合，构建强大且响应迅速的基础架构，以应对新出现的挑战。

增强安全性的战略合作伙伴关系

戴尔与 Microsoft、CrowdStrike 和 Secureworks 等网络安全领导者携手合作。每项合作关系都可增强戴尔的解决方案，为客户提供卓越的保护功能，如高级威胁情报、端点监控和全面的响应战略。

利用 Dell Professional Services

Dell Technologies 的专业服务可提供专业知识和指导，帮助企业有效应对复杂的网络安全挑战。从制定事件响应计划到实施零信任体系结构，戴尔专家确保客户端环境能够抵御备份渗透等现代威胁。

携手戴尔，构建业务弹性

选择 Dell Technologies，让企业能够战胜复杂攻击者，同时保持运营连续性。通过创新、合作伙伴关系和专业知识，戴尔确保组织能够预防、检测极其严重的备份渗透攻击并快速恢复。

后续行动

立即联系 Dell Technologies，保护您的业务安全无虞。与我们携手合作，我们将共同守护您的关键资产、维护您的声誉，并为您打造一个充满弹性的未来。

戴尔始终致力于培养对数字时代的信心，为组织提供安全运营和蓬勃发展所需的工具、知识和支持。

备份弹性 — Dell Technologies 护航，智启新程。立即行动，让您的运营无忧，并树立对网络安全态势的信心。

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