DELL Technologies

零日攻击防护：Dell Technologies 助力提高网络安全和弹性

零日攻击威胁不断增加

零日攻击已迅速升级为当今网络安全环境中最严峻的一大挑战。这类攻击利用软件提供商和安全专家未知的漏洞，使企业毫无防备并面临风险。从医疗到金融等各行各业的企业都容易遭受此类攻击，这些攻击通常会导致严重的财务和运营后果。

随着数字化转型的步伐加快，零日攻击变得更加频发且复杂。如今，企业对强大防护的需求更甚于以往。Dell Technologies 深知此类威胁的严重性，并为企业提供创新且可扩展的防护方案，助力企业有效应对零日攻击并实现快速恢复。

零日攻击是什么？

零日攻击是指攻击者在修补程序或补丁程序推出之前，攻击软件或硬件中未公开的安全漏洞。攻击者通常会利用这个窗口期趁虚而入，在企业发现并解决漏洞之前造成大规模的业务中断。

零日攻击原理剖析

1. **发现漏洞：** 黑客识别软件应用程序或系统中存在的编码缺陷或隐藏后门。
2. **开发利用程序：** 制作恶意软件，用于攻击特定漏洞。攻击者可能会通过定向网络钓鱼活动或携带恶意软件的网站来投放攻击程序。
3. **发起攻击：** 部署漏洞利用程序，从而入侵系统，并可能导致数据失窃或运营中断。

常见技术

- 偷渡式下载会诱使用户在不知情的情况下安装恶意软件。
- 网络钓鱼电子邮件通过分发恶意链接或恶意程序来利用漏洞。
- 无文件攻击通过将恶意操作完全在系统内存中执行，从而规避检测。

这些高度复杂的攻击载体使得零日攻击变得极其危险，因为传统的基于特征码的检测工具往往无法识别它们。

对企业的影响

由于其不可预测性和检测上的延迟，零日攻击带来了巨大的风险。其造成的后果可能在多个层面产生灾难性影响。

财务损失

零日攻击一旦得逞，可能会引发巨大损失，包括监管机构罚款和停机期间的收入损失。例如，当电子商务平台中的未知漏洞被利用时，可能会导致结算功能瘫痪，从而直接影响销售。

声誉后果

企业的声誉可能会受到无法挽回的损害。当敏感信息泄露或服务中断时，客户信任度将严重受损。

运营中断

未被修复的漏洞常常会导致系统瘫痪，进而造成工作效率骤降、项目延误和商机流失。

现实案例

一家大型医疗机构曾遭受零日攻击，攻击目标是未打补丁的医疗设备软件。此次攻击不仅导致关键业务中断、患者数据泄露，还使得该机构付出了**数百万**美元的恢复成本，更严重的是损害了患者信任。

警报统计信息

根据 Ponemon 研究所 2023 年的一项研究，大约 80% 的数据泄露事件与零日漏洞有关

在所有被攻击的漏洞中，

零日攻击漏洞的占比一直超过 **70%**

资料来源：《2024: IMandiant “M-Trends”》

Dell Technologies 助力抵御零日攻击

Dell Technologies 提供业界卓越的解决方案，可帮助企业积极抵御零日攻击，同时还能使其在遭受攻击后快速实现业务恢复。

服务器和存储安全解决方案

戴尔的服务器与存储安全解决方案提供多重额外防护保障：

- 安全服务器会监控并阻止未经授权的访问尝试。
- 即使在最糟糕的情况下，数据备份和恢复系统仍可确保关键信息能够访问且完好无损。

戴尔可信设备助力强化端点

端点是攻击者入侵的关键切入点。戴尔可信设备内置先进安全机制，能确保端点即使面对未发现的威胁也能持续受到保护。

- **SafeBIOS** 技术可保护固件免遭篡改，从根本上确保系统的完整性。
- **SafeID** 通过确保身份验证过程的安全性来保护用户凭据。
- **SafeData** 技术会对静态和传输中的敏感数据进行加密，确保数据在被截获或窃取后对攻击者毫无价值。

借助 CrowdStrike 实现主动威胁检测

CrowdStrike 运用高级分析与 AI 技术监视端点活动，有效检测可能预示零日攻击的异常行为。其主动威胁检测功能可确保在漏洞导致大范围损害之前迅速做出响应。

例如，某电信运营商通过使用 CrowdStrike，得以及早检测到网络流量异常，进而成功缓解了客户服务器上潜在的零日攻击风险。

Dell PowerProtect 解决方案

Dell PowerProtect 可实现稳健可靠的不可变备份，并提供安全的隔离恢复方案。在遭受零日攻击后，企业可以快速高效地恢复运营，从而维护业务连续性并保护重要的客户数据。

例如，某大型零售连锁企业利用 PowerProtect 成功恢复了因零日漏洞导致勒索软件攻击而遭加密的文件，从而避免了业务长期中断。

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

在整个基础架构中实现高级网络分段、严格的访问控制和实时流量分析，有效增强针对零日攻击的防御能力。

采用多层安全方法的重要性

真正的安全保障需要多重解决方案。多层防御策略通过融合技术、流程和人员三大要素，构建起全方位的保护框架。

强化防御体系的关键举措

- **采用零信任原则：**对所有尝试接入网络的个体与设备进行验证。
- **实施高级加密：**利用加密协议来保护传输中的数据和静态数据。
- **开展员工培训：**通过详细培训课程教导员工识别网络钓鱼手段与社会工程学攻击手法。
- **定期测试系统：**通过持续的渗透测试与漏洞扫描，确保防御体系持续适应新型威胁。

Dell Technologies 将这些实践与其先进安全解决方案相结合，确保各企业能够有效应对零日漏洞威胁。

强化网络安全的合作伙伴关系

戴尔与业界领先企业 **Microsoft**、**CrowdStrike** 和 **Secureworks** 携手合作，为客户提供前沿的安全情报和先进的工具。

- **Microsoft** 与戴尔解决方案实现无缝集成，确保提供系统级的全面兼容性与主动式防护机制。
- **CrowdStrike** 提供高级端点威胁情报，以检测潜在的零日漏洞攻击。
- **Secureworks** 提供持续监控与专家级修复服务，实现实时攻击响应。

利用 Dell Professional Services

Dell Professional Services 提供涵盖咨询、实施与恢复支持的全方位服务，助力企业应对并降低零日威胁相关风险。从事件应急响应到网络安全路线图规划，戴尔助力各企业实现长期的业务弹性。

打造弹性未来

选择与 Dell Technologies 携手合作，意味着您获得的不仅是卓越的技术，更是安心的保障。戴尔通过先进的解决方案、战略合作伙伴关系及卓越的专业能力，赋能各企业有效预测、检测高度复杂的零日攻击并成功进行恢复。

立即联系 Dell Technologies，筑牢企业安全防线，守护品牌声誉，在充满不确定性的数字环境中稳健发展。选择戴尔，为您的未来保驾护航，无惧明日威胁挑战。

Dell Technologies 通过专为保护关键资产而设计的安全解决方案与服务激发企业信心，使其能够在应对不断变化的零日攻击挑战中始终领先一步。

如需了解如何应对当今重大的网络安全挑战，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