DELL Technologies

勒索软件防护：Dell Technologies 助力提高网络安全和弹性

勒索软件是什么?

勒索软件是一种恶意软件，它通过锁定计算机系统或数据来阻止用户访问，并要求用户支付赎金后才能恢复。它是最具破坏性的网络攻击类型之一。全球有 50% 的企业在过去一年中至少遭受过一次勒索软件攻击，勒索软件攻击后的平均停机时间为三周，这会导致严重的运营中断

勒索软件威胁不断上升

勒索软件是一种恶意软件，它通过锁定计算机系统或数据来阻止用户访问，并要求用户支付赎金后才能恢复。它是最具破坏性的网络攻击类型之一。全球有 50% 的企业在过去一年中至少遭受过一次勒索软件攻击，勒索软件攻击后的平均停机时间为三周，这会导致严重的运营中断。

勒索软件的攻击原理

当用户单击恶意链接、打开受感染的附件或访问被入侵的网站时，勒索软件通常会感染用户所在组织。随后，它会侵入系统对文件进行加密，使其无法被读取。此后，勒索软件程序通常会向用户发送消息，要求支付赎金（通常以加密货币形式）以换取解密密钥。在未支付赎金的情况下，攻击者可能会威胁删除数据或公开泄露数据。2017 年爆发的 WannaCry 攻击就是一个典型的勒索软件攻击案例。它在全球范围内迅速蔓延，波及了医院、企业和政府机构，并造成了巨大的经济损失。根据 Cyber Risk Management (CyRiM) 和伦敦劳合社的数据，WannaCry 病毒在短短几天内就波及了 150 个国家，影响了超过 20 万台系统，其造成的全球经济损失在 40 亿至 80 亿美元之间。

在全球受影响的大型公司中，有两家分别是 FedEx 和 Renault-Nissan。前者宣称因服务中断和善后清理，其损失达 3 亿美元，而后者则被迫暂时关闭了数家工厂的生产线。勒索软件攻击的隐性成本可能涉及多个方面，例如：

- 企业运营中断与生产力损失
- 声誉受损
- 系统恢复与漏洞修补成本
- 法律与监管罚金

面临勒索软件攻击时，企业应采取以下步骤；

- 除非绝对必要，否则不要支付赎金，因为攻击者无法保证您能够恢复访问。
- 如果存在备份，请通过备份进行恢复。
- 向当局报告攻击事件。
- 加强防御措施，以防止未来让攻击得逞（例如，及时更新软件、对员工进行培训、采用端点保护措施）。

借助 Dell Technologies 防护勒索软件攻击

Dell Technologies 为企业提供全面且富有前瞻性的工具，旨在帮助企业在勒索软件造成损害前有效遏制相关风险。

通过戴尔可信设备增强端点安全性

端点通常是勒索软件攻击的主要入口，因此端点安全成为重要的关注领域。戴尔可信设备集成了基于硬件的安全功能，可在不影响性能的情况下保护系统。Dell SafeBIOS 和 SafeID 等解决方案可增强端点设备的安全性，以防止未经授权的访问；而 Dell SafeData 则会对数据进行加密，从而确保即使在企业防火墙之外也能保护敏感信息。通过将安全特性直接集成到设备中，企业可以实现硬件级别的防护，让攻击者更难有机可乘。

借助 CrowdStrike 实现主动检测

如果企业使用合适的工具实时检测和响应威胁，勒索软件攻击并非不可避免。戴尔解决方案组合中包含 CrowdStrike，它提供了基于 AI 和行为分析的新一代端点保护平台。该技术能够发现并阻止可疑活动，防止其演变为攻击。通过与戴尔基础架构无缝集成，CrowdStrike 使 IT 团队能够保持对整个环境的可见性，并实现即时有效的威胁响应。

Dell PowerProtect 提供全面的数据保护

Dell PowerProtect 解决方案是应对勒索软件风险的关键支撑。这些高级数据保护工具旨在保护企业数据免受内部和外部威胁的影响。不可变备份等功能可确保您的数据不会被勒索软件篡改、删除或加密，即使面对高级攻击也能提供可靠的安全保障。以 Dell PowerProtect Cyber Recovery Vault 为例，它利用物理隔离技术将关键数据与网络隔离，确保即使在高度复杂的网络攻击中，数据也能保持原样，不受侵扰。通过自动化异常检测和智能工作流，企业能够及早检测到恶意活动并在勒索软件蔓延之前做出响应。

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。

Dell Data Protection Services 助力实现大规模恢复

戴尔深知，虽然预防能力至关重要，但恢复能力也是勒索软件防护中同等重要的一个方面。Dell Data Protection Services 不仅提供自动化备份和恢复解决方案，还提供专家主导的咨询服务，以确保企业能够快速恢复并尽可能减少停机时间。Remote Data Recovery 和 Incident Response 等服务可确保企业在危急关头获得所需的支持。这种全面的方法可确保数据完整性得以保留，并缩短恢复时间，从而防止业务中断。

这只是戴尔解决方案组合中的一些示例，用于帮助您应对内部恶意威胁。

通过合作伙伴关系实现优势

戴尔还积极与其他公司合作，因此我们所提供的保护并非只局限于自身所拥有的技术。通过与 CrowdStrike 和 Secureworks 等卓越网络安全公司合作，戴尔提供了一个集成式解决方案生态系统，可应对各种途径的攻击。这些解决方案将共同提供端到端的安全防护，使企业能够根据其特有的风险状况构筑多层防御。

为何选择戴尔?

Dell Technologies 不仅仅是一家技术提供商，更是在防护勒索软件攻击方面值得信赖的合作伙伴。戴尔将创新、专业知识以及为企业赋能的承诺相结合，可为各企业提供应对不断变化的威胁所需的工具和信心。无论是保护端点、保护关键数据，还是实现快速恢复，戴尔的产品和服务都能确保运营连续性，让您安心无忧。

构建富有弹性的未来

勒索软件攻击不断演变，但 Dell Technologies 可助力企业始终先人一步。利用先进的硬件、软件和服务，各企业可以构建富有弹性、适应性强且安全可靠的网络安全框架。立即借助戴尔全面的防勒索软件解决方案，保护您的数据，保障您的运营，为业务的未来发展奠定基础。

为确保业务的弹性，了解当前的威胁态势并随时掌握新兴威胁信息至关重要。Dell Technologies 的网络安全专家会持续监控新的攻击途径（我们的称呼方式），并着力于主动解决我们产品和服务中存在的潜在漏洞。这使我们能够为您提供前沿防护措施，防范不断发展的勒索软件威胁。

除了及时了解信息，各企业还必须采取多层次的安全措施。这意味着要部署一系列安全措施，例如防火墙、反恶意软件、入侵检测系统和数据备份。通过采取多元化的防御策略，您能有效降低单次攻击造成的影响，并确保即便勒索软件入侵得逞，您的业务也能保持运行。

定期测试和更新安全措施（包括修补系统和更新策略）也很重要。黑客一直在寻找绕过传统安全措施的新方法。因此，企业必须通过定期测试并根据需要更新自身防御措施，以保持领先地位。该计划包括定期进行漏洞评估、渗透测试和补丁管理。

保护您的业务免受勒索软件侵害的另一个关键方面，是对您的员工进行网络安全最佳实践培训。许多勒索软件攻击都是通过网络钓鱼电子邮件或恶意链接等社会工程手段发起的。让员工了解如何发现和避免这些威胁，可以大幅降低攻击得逞的可能性。

此外，制定灾难恢复计划可以显著减轻勒索软件攻击的影响。该计划应包括对重要数据和系统进行定期备份，以及制定明确的攻击响应和恢复流程。

除了这些主动预防措施之外，制定一份完善的事件响应计划也同样重要。这包括明确的应对勒索软件攻击的角色和责任，以及用于通知利益相关方和减轻损失的沟通机制。

最后，了解勒索软件攻击的最新趋势和发展动态可以帮助您未雨绸缪，提前防范潜在威胁。通过定期审阅行业报告和安全专家的更新信息，您可以主动实施新的安全措施来保护您的业务。

任何企业都无法完全避免受到勒索软件的攻击，但通过部署恰当的策略和工具，您可以大幅降低此类攻击带来的风险和影响。通过采取积极主动的网络安全方法，您不仅可以保护自己的业务，还能赢得客户和利益相关方的信任。

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