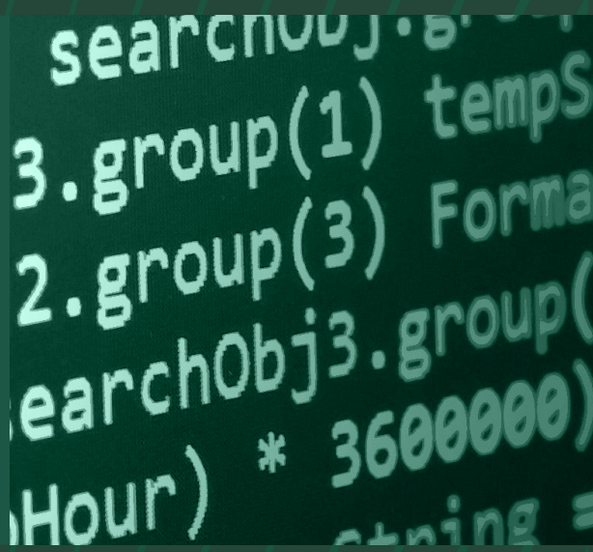
DELL Technologies

5 对于安稳度过勒索软件攻击的建议



1 维护好全面的事件响应计划

想方设法减少攻击的影响

经常练习、测试和更新

提前安排好事件响应团队

将网络保险作为整体抗风险策略的一部分

拟定与执法部门的合作计划

2 制定清晰的沟通策略

提前创建沟通模板

确保组织内能够及时、清晰地进行沟通

为对外沟通做好准备（如果适用）

遵守适用的通知法规

3 提供强大的数据保护

使用独立、不可变且安全隔离的数据存储区保护关键数据

按服务/基础架构确定恢复的优先顺序

对恢复流程进行演练

配备“洁净室”等功能，以满足您的恢复时间目标

确保可恢复数据的完整性

4 不要想着能立即恢复正常

支付赎金是万不得已的无奈之举

付款前，请确保遵守法律和法规要求

即使支付了赎金，也不能保证黑客会归还您的数据

5 重视培训和教育

进行模拟攻击

监控和测试员工在涉及安全性方面的做法

使用网络钓鱼测试和电子邮件安全培训等工具

遭受攻击已无可回避，只是早晚问题。

即便企业已经筑起强有力的防御工事，也必须为不可避免的攻击做好计划。戴尔主题专家 — 网络安全与合规实践部全球总监 Jim Shook、网络安全解决方案和战略合作关系部首席顾问 Steven Granat 与 Dell Data Protection 产品营销高级顾问 Brian White 齐聚一堂，就如何应对灾难展开了讨论。

> 您需要安排合适的人员，进行演习并模拟攻击，这样当攻击发生时，每个人都能立即就位，知道自己要做什么。”
>
> ***Steven Granat，** Dell Technologies 网络安全解决方案和战略合作关系部首席顾问*

维护好全面的事件响应计划

受到攻击时，所有关键利益相关者（组织中的几乎每个人以及供应商等第三方）都必须知道该怎么做。Shook 认为，应该制定书面事件响应计划，明确行动顺序。全面的计划要涵盖从即时行动到恢复阶段的技术、流程和沟通步骤。此外，一定要保留纸质书面文档，因为数字模式的通信可能会无法实行。“您需要一个可以随时从书架上拿下来参考的计划。”Granat 说。

制定清晰的沟通策略

大多数组织都需要与主要利益相关者进行沟通，而且许多情况下还需要遵守法规要求。为内部和外部创建不同的通信模板，系统性地说明在何时按什么顺序通知哪些人。要为电话和电子邮件系统崩溃的情况做好准备。

实施强大的数据保护策略

度过勒索软件攻击的一个关键目标是尽可能轻松地还原数据并恢复运营，而又不用支付赎金。强大的数据保护策略是实现这些目标的关键，但需要得到技术和流程这两方面的支持。“使用不可变数据和网络存储区存储的各种数据，可以作为可信赖的数据用于恢复系统，或至少用于系统恢复时的点式验证，”Shook 建议道。确保数据受到保护是第一步；您还必须拥有合适的人员和流程来开展恢复工作。第三方专家可以提供帮助，但他们在规划阶段就应该参与进来。

即时支付了赎金，也不要以为能立即恢复正常

支付赎金是万不得已的无奈之举，并不能保证组织运营能够立即恢复如常。不要忘了，您正在与犯罪分子谈判，即使您真的获得了解码器密钥，也需要为新恢复的数据制定好策略。首先，您必须测试解密的数据并有条不紊地重建所有系统。在攻击发生之前反复进行细致的假设分析，将大大有助于建立抗风险能力。“了解技术基础架构中的不同应用程序和依赖关系对于高效恢复稳定状态至关重要。‘我是否有可用的恢复源和可用于恢复的目标？’‘我是否拥有未受损坏的数据？’这些都是需要考虑的重要因素。”Granat 说。

在恢复阶段，您还需要确保对手真的已经离开了您的系统。“就像火灾一样。发生火灾后，您需要第一时间确保火已经彻底扑灭，还要找出引发火灾的原因。如果没有这两项关键信息，您未来仍会面临被攻击的风险。”Shook 说。

培训和练习至关重要

网络弹性的重要一环是全面培训，从确保员工实施严格的网络安全措施，到定期按恢复计划进行演练，涉及方方面面。“您需要安排合适的人员，进行演习并模拟攻击，这样当攻击发生时，每个人都能立即就位，知道自己要做什么。”Shook 说。

在如今的威胁环境下，勒索软件可以说是防不胜防，但通过规划和执行，您可以尽可能减少对运营、财务和声誉的影响。我们的目标就是尽量快速轻松地重回正规。

了解如何应对当今一些主要的网络安全挑战：**dell.com/cybersecuritymonth**

DELL Technologies