医疗保健机构在遭遇勒索软件攻击后能够更快速地恢复

一家大型医疗保健机构使用 Quest Recovery Manager for Active Directory Disaster Recovery Edition，确保在深夜遭遇勒索软件攻击后恢复正常运行。

大型医疗保健机构

员工数： **25,000**

行业： **医疗保健**

简介

几年前，一家大型医疗保健机构的 IT 团队成员在夜间收到警报，获悉其 Active Directory 环境中出现可疑活动。经过数小时的调查后，他们发现机构受到勒索软件攻击。

团队迅速赶往现场开始恢复流程，但遇到各种问题，导致恢复工作暂时无法开展。

业务发展导致恢复能力有所欠缺

机构经历过多次合并和收购。尽管他们已使用 Quest Recovery Manager 备份了其部分环境，但在组织的快速变更之中，此工具已递交给新的管理员，而部分林尚未经过备份。此外，公司没有制定全面的业务恢复计划，这意味着机构处于离线状态，使得在医院和异地持续提供患者护理服务的任务更为繁重。该

挑战

遭遇勒索软件攻击后，机构需要恢复；为此，机构的 IT 团队需要判断环境的哪些部分已得到备份，哪些部分需要完全重建，以及如何及时将受感染的部分从系统中清除，以使医疗保健运营尽可能不受影响。

解决方案

Quest Recovery Manager for Active Directory Disaster Recovery Edition 确保了该机构的主林得以备份且能够在一天之内恢复。

成果或益处

- 患者护理有保障，业务职能得以快速恢复
- 完全备份的环境，可在一天之内恢复
- 通过深度网络抗风险能力消除风险

机构 IT 安全团队的前成员表示，“即使这些公司有了工具，但他们仍缺少计划，IT 和 Active Directory 管理员不仅有责任确保制定灾难恢复计划，还要负责制定业务计划。”

缺乏恢复计划导致他们面临一项重大问题：IT 管理员别无选择，只能等着机构的业务部门来确定任务优先级、程序和协议。然而，这个过程需要一段时间，因为机构的法务部门及其他部门也需要参与其中。另一位前员工评论道：“我认为，作为一个机构，我们未能从业务方面做好充分准备，以致无法真正地快速启动恢复程序，以致耽误时间，无法及时恢复上线和使环境重回正轨。”

争分夺秒。机构的环境处于离线状态和 Active Directory 访问权限遭到入侵的每一分钟，员工都需要使用纸笔来维护关键操作并确保患者护理不受影响。机构需要恢复解决方案，并且该解决方案需要能够快速恢复环境。

> “这种情况下，Quest 可提供的协助显得尤为重要，因为每个人都在争先恐后地试图弄清楚从何着手。”
>
> *前员工*

Quest 可减少恢复时间和精力

可喜的是，该机构已投资采用 Quest Recovery Manager Forest Edition 来备份他们规模最大的 Active Directory 林，并且已实施妥善做法。当 Quest 收到该机构面临灾难的警报时，会立即将此解决方案升级到 Disaster Recovery Edition，并提供专家指导，助他们度过危机。结果是，Disaster Recovery Edition 帮助 IT 在一天之内恢复了相关的林，其自动化功能不仅缩短了恢复时间，而且提高了准确性。这些前员工表示，该解决方案的自动化功能“甚至涵盖了我们都不知道需要完成的步骤。我甚至无法想象自己如何坐在那里执行所有这些步骤，并阅读相关文章来了解怎样以原生方式完成这些任务。”

为了恢复未能使用 Recovery Manager 备份的另外四个林，多个至少由两三人组成的 IT 团队均花费了数天时间来完成此流程，因为他们需要从头重建这些林。

为避免再次受到感染，Quest 为该机构提供了多项能力，让他们能够对遭到入侵的特权组帐户进行重置、创建新的管理密码以及强制重置特权组。有了深度防御措施，窃取凭据的网络罪犯便无法再使用这些被窃的凭据。

> “对我们来说，这件事是一次痛苦的经历。”
>
> *前员工*

汲取的经验

回望勒索软件带来的严峻考验，IT 和安全从业人员为其他机构提供了下列建议，以避开陷阱并在发生灾难后尽快恢复运营：

- 不要等到灾难发生后才制定兼顾技术和业务两个方面的恢复计划。您需要尽快开始恢复，并降低业务所受的影响；例如，停机期间的收入损失、加班成本和重新分配预算都可能妨碍开展基本服务，例如第三方取证。
- 针对网络离线模式等场景下进行桌面演习，让每个人都能理解应用程序和服务的执行方式。此演习应包括业务部门和 IT 部门应如何响应，以做出及时且明智的决策。

- 将灾难恢复计划和卓越技术视为保险手段。您或许希望永远不要用到它，然而行业趋势显示并非如此。拥有综合全面且经过演练的灾难恢复计划，您和您的同事便可高枕无忧，因为在发生灾难时，无论是源于小错误，亦或遭遇全面的勒索软件和勒索攻击，您的团队都已做好应对准备。
- 为恢复所需的更多存储空间制订预算。在您机构进行恢复期间，您需要留出受感染的区域进行取证及其他审查，以了解作案者的作案方式；与此同时，您需要努力创建新的环境。很多机构在尝试恢复环境时并不会想到环境规模会增加，但事实的确如此，这一点需要谨记在心。
- 如果正值进行公司并购，请确保在做出 IT 预算决策之前，对新加入机构的备份和恢复工具进行评估，以确保哪怕这些工具过时或不足，仍有资金可用。

“这种情况下，Quest 可提供的协助显得尤为重要，因为当每个人都在争先恐后地试图弄清楚从何着手时，我们会安排一位 Quest 人员完全专注于处理这一件事情。‘除非如此，否则什么也做不了，因此让我们就此开始吧。我们慢慢地开始恢复，然后继续下去。’这太棒了。”

产品及服务

解决方案

- Recovery Manager for Active Directory Disaster Recovery Edition

关于 Quest

Quest 提供软件解决方案，在日益复杂的 IT 环境中带来新技术的优势。从数据库和系统管理到 Active Directory 和 Microsoft 365 迁移和管理，以及网络抗风险能力，Quest 都可帮助客户在当下解决其面临的下一个 IT 挑战。Quest Software。Where Next Meets Now.