ConversationalGeek

Microsoft Teams 备份信息图表

作者：Brien M. Posey，Microsoft MVP

#1 确保您正在备份 Microsoft Teams

第一项 Microsoft Teams 备份最佳实践其实很简单，即确保您确实在备份 Microsoft Teams（以及其他 Microsoft 365 应用）。

Office 365 的第三方备份增加了 18 个百分点，从 2020 年的 27% 跃升至 2021 年的 45%
http://vee.am/DPR21report

Netwrix Research 的数据显示，人为错误造成的数据丢失最多，占比达 50%
https://hostingtribunal.com/blog/data-loss-statistics/#gref

Netwrix Research 的数据显示，35% 的数据丢失是因为硬件故障
https://hostingtribunal.com/blog/data-loss-statistics/#gref

#2 采用真正了解 Teams的备份解决方案

与 Exchange Online 或 SharePoint Online 等应用程序不同，Teams 不会将所有数据存储在一个位置，而是分散在多个不同的 Microsoft 365 应用程序中。虽然任何 Microsoft 365 备份应用程序均应能够备份 Teams 数据，但除非该应用程序是专为支持 Microsoft Teams 而设计的，否则还原流程可能会非常困难。

Tech Radar 指出，“据 Tech Radar 报道，Microsoft 在 2021 年 7 月透露，其 Teams 的月活跃用户数量达到 2.5 亿。这比同年 4 月报告的 1.45 亿增加了 1 亿多
https://www.techradar.com/news/microsoft-teams-now-has-250-million-monthly-active-users

“超过 500,000 个组织使用 Microsoft Teams 作为其默认讯息平台”
https://www.businessofapps.com/data/microsoft-teams-statistics

#3 在任务中使用合适的工具

第三项 Microsoft Teams 备份最佳实践是确保您在作业中使用合适的工具。Microsoft 365 生态系统中的某些特性（例如保留策略和诉讼保留）可以充当伪备份。但这些工具用于合规目的，而非数据保护。因此，它们不能为 Microsoft Teams 数据提供充分保护。

60%
根据 Avast 的数据，“60% 的备份是不完整的”。这主要是因为公司使用过时的备份技术
https://invenioit.com/continuity/disaster-recovery-statistics

37%
37% 的中小型企业遭遇过云端数据丢失
https://invenioit.com/continuity/disaster-recoverystatistics

#4 采用混合备份方法

第四项最佳实践是采用混合备份方法。最好使用可以同时保护两个环境的单个备份应用程序，而非将 Microsoft 365 与内部 Microsoft Office 应用程序分开备份。

备份正从内部转向由服务提供商管理的基于云的解决方案，后者的占比预计将从 2020 年的 29% 增长到 2023 年的 46%

在未来两年内，大多数企业希望逐步减少物理服务器，维持和加强虚拟化基础架构，并拥抱“云为先”战略。这意味着到 2023 年，一半的生产工作负载将托管在云端。

https://solutionsreview.com/backup-disasterrecovery/veeam-data-protection-report-2021-shows-58-of-backups-are-failing

#5 确保 SLA 成为备份计划的首要任务

第五项最佳实践是确保服务等级协议 (SLA) 成为备份计划的首要任务。具体而言，您需要考虑适合您的 Microsoft Teams 环境的恢复点目标 (RPO) 和恢复时间目标 (RTO)。RPO 将确定备份创建频率，从而确定备份之间可能丢失的最大数据量。RTO 表示备份还原所需的时长。

80%
80% 的组织认为，他们的实际应用程序恢复速度与预期速度存在“可用性差距”

76%
这些组织中有 76% 表示其数据备份频率与其可以承受的丢失数据之间存在差距

#6 切勿忽视恢复细粒度

一项往往被忽视的 Microsoft Teams 备份最佳实践是确保您所用的备份解决方案支持细粒度恢复功能。尽管能够还原整个团队（甚至多个团队）很重要，但能够还原团队内的文件或聊天信息也同样重要。

44% 的 SaaS 管理员和 47% 的备份管理员将改进还原功能（包括细粒度还原）列为其保护 Office 365 数据的主要措施
https://www.youtube.com/watch?v=RIHm8-0LUJs

2020 年，70% 的财富 500 强公司购买了 Office 365
https://hostingtribunal.com/blog/microsoft-statistics/#gref

#7 使用备份来增强 eDiscovery 功能

Microsoft 365 长期以来一直提供 eDiscovery 功能，支持组织根据传票从 Microsoft 365 生态系统中定位特定数据。尽管原生 eDiscovery 功能有其作用，但在发现流程中使用备份软件通常更有效。

一项“eDiscovery 中断”调研发现，“至少 58% 的受众曾‘多次’使用 eDiscovery 技术处理不涉及索赔或争议的问题。”这说明 eDiscovery 不再仅限于诉讼

$12.9 Billion
到 2025 年，eDiscovery 市场预计将增长到 129 亿美元

*https://ediscoverytoday.com/2020/08/31/here-are-some-disruptivestats-in-discovery-ediscovery-trends

**https://www.prnewswire.com/newsreleases/global-12-9-billion-ediscovery-market-forecast-to-2025---focus-on-proactive-governance-withdata-analytics-and-the-emergence-of-new-content-sources-301231643.html

#8 保护 Teams 免遭勒索软件的侵害

另一项最佳实践是切实保护 Microsoft Teams 数据免受勒索软件的侵害。与普遍的看法相反，存储在 Microsoft 365 中的数据可以被勒索软件加密。许多人仍然通过个人设备远程办公，这大大增加了勒索软件感染的风险。妥善的备份是防范勒索软件相关数据丢失的最佳防御方法。

Ponemon Institute 的数据显示，仅45% 的企业认为他们拥有足够的网络安全预算

IDC 的数据显示，12 个月内有 69% 的组织被恶意软件攻击突破防线，其中 39% 涉及勒索软件

*https://www.keeper.io/hubfs/PDF/Cybersecurity%20in%20the%20Remote%20Work%20Era%20-%20A%20Global%20Risk%20Report.pdf)

**https://www.veeam.com/why-backup-office-365.html

#9 确保您的存储提供灵活性

在为 Microsoft Teams 选择备份应用程序时，请务必确保解决方案支持您自由选择自己的存储，无论该存储位于何处。这样，组织便可选择以最低成本提供业务所需的性能和弹性的存储层。存储灵活性还能够让组织按需选择将备份写入不可变存储，从而保护备份免受勒索软件攻击。

CAN Financial 在 2021 年支付了 4000 万美元的赎金，创下了世界记录

Sophos 在 2021 年开展的一项调研发现，“7% 受访者的组织在去年受到勒索软件的攻击”

*https://www.businessinsider.com/cna-financial-hackers-40-million-ransom-cyberattack-2021-5).

**https://www.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-ofransomware-2021-wp.pdf?cmp=120469

#10 注重易用性

一些备份应用程序配置和使用过于复杂。问题在于，复杂性增加了人为错误的几率。如果组织选择直观易用的备份应用程序，则可降低因人为错误所致的备份或恢复失败的几率。

FEMA 的数据显示，40-60% 的小企业在数据丢失事件后彻底倒闭
https://hostingtribunal.com/blog/data-loss-statistics/#gref

2021 年的一项研究显示，58% 的备份未能还原
58%

*https://www.continuitycentral.com/index.php/news/technology/6092-survey-finds-that-58-percent-ofdata-backups-fail-when-restoration-is-attempted

ConversationalGeek

赞助方：
VEEAM 徽标