Os 7 Motivos Críticos para Fazer Backup do Microsoft 365

Os motivos pelos quais as organizações precisam proteger os dados do Microsoft 365

Introdução

Você tem o controle dos seus dados do Microsoft 365? Você tem acesso a todos os itens dos quais precisa? A reação instantânea normalmente é "claro que sim" ou "a Microsoft cuida disso tudo". Mas parando para pensar, você tem certeza?

A Microsoft cuida de muita coisa. Eles fornecem um ótimo serviço para seus clientes, gerenciando a infraestrutura do Microsoft 365 e mantendo o tempo de atividade para os seus usuários. Mas, por outro lado, eles estão dando a VOCÊ a responsabilidade sobre os seus dados. Há um equívoco comum em pensar que, por padrão, a Microsoft faz o backup de seus dados por você, mas o backup completo não está incluído em uma licença padrão do Microsoft 365. Sem uma mudança de mentalidade, pode haver repercussões danosas quando essa responsabilidade é deixada de lado.

No fim das contas, você precisa garantir o acesso e o controle sobre seus dados do Exchange Online, SharePoint Online, OneDrive for Business e Microsoft Teams. Além disso, mesmo que você não queira gerenciar a infraestrutura de backup, existem serviços de backup que são implantados rapidamente, sem a necessidade de gerenciamento ou manutenção manual contínua. Pense no acesso instantâneo a proteção de dados personalizável, na recuperação ultrarrápida e na confiança de que você está sempre no controle. Agora pense no que você está arriscando por não tê-los.

Esse relatório explora os perigos de não ter um plano de backup do Microsoft 365 em seu arsenal. Falaremos sobre como as soluções de backup para o Microsoft 365, particularmente os serviços de backup baseados na nuvem, preenchem a lacuna da retenção de longo prazo e da proteção de dados e são realmente cruciais para as empresas modernas.

> "A Sun Chemical é um negócio verdadeiramente global: Todos os dias, funcionários espalhados pelo mundo confiam nas aplicações do Microsoft 365 para trocar dados essenciais. O Veeam Data Cloud for Microsoft 365 protege essa parte essencial do nosso ambiente, ajudando nossos funcionários a trabalhar mais produtivamente e nos dando uma camada extra de resiliência cibernética."

Stuart Hudson
Gerente Sênior de Infraestrutura Global de TI
Programas Estratégicos de Infraestrutura — AP, Sun Chemical

O grande equívoco sobre o Microsoft 365

O engano se dá entre a percepção da responsabilidade da Microsoft e a realidade da responsabilidade do usuário quanto à proteção e à retenção em longo prazo dos seus dados do Microsoft 365. A resiliência e a retenção oferecidas pela Microsoft em uma licença padrão do Microsoft 365 e o que os usuários presumem receber geralmente são diferentes. Ou seja, além das precauções padrão que o Microsoft 365 dispõe, talvez você precise reavaliar o nível de controle que tem sobre seus dados e quanto acesso realmente tem a eles.

O Microsoft 365 oferece redundância geográfica, que costuma ser confundida com um backup. A redundância geográfica protege contra falha de hardware ou de site, então se houver algum tipo de paralisação ou pane de infraestrutura, seus usuários permanecerão produtivos e alheios a esses problemas subjacentes. Os backups, por outro lado, acontecem quando uma cópia histórica dos dados é feita e então armazenada em outro local, separado do ambiente de produção. Isso garante que uma cópia dos seus dados exista, independentemente do que aconteça com o Microsoft 365, e que a opção de recuperação esteja sempre disponível.

Os backups, mais do que a redundância geográfica, são a última linha de defesa de uma empresa, mas tão importante quanto tê-los é garantir acesso direto a eles e controle sobre eles. Quando os dados são perdidos, excluídos acidentalmente ou atacados de forma maliciosa, você precisa ter certeza de que pode recuperá-los rapidamente.

O Microsoft 365 é uma responsabilidade compartilhada

> "Para todos os tipos de implantação em nuvem, você é o proprietário de seus dados e identidades."

Fonte: Responsabilidade compartilhada na nuvem, Microsoft

7 Motivos pelos quais um Plano de Backup do Microsoft 365 É Essencial

Como uma plataforma robusta e de alta capacidade de software como serviço (SaaS), o Microsoft 365 se encaixa perfeitamente nas necessidades de muitas organizações. O Microsoft 365 fornece tempo de atividade e disponibilidade de aplicações para garantir que os seus usuários não percam tempo. Mas uma solução de backup abrangente pode proteger você contra muitas outras ameaças de segurança, fornecendo tranquilidade e uma proteção de dados robusta.

Talvez você ou seu chefe pensem: "A lixeira já dá conta de recuperar o que for preciso". É aí que muitas pessoas se enganam. O tempo médio de demora entre o comprometimento de dados e sua descoberta pode chegar a 140 dias, uma lacuna chocantemente grande. É muito provável que você não perceba que alguma coisa está faltando ou foi perdida até que seja tarde demais para a lixeira — e isso está longe de ser o problema mais urgente.

Conversamos com centenas de profissionais de TI de todo o planeta que migraram para o Microsoft 365 e, a partir de suas percepções, sete vulnerabilidades na proteção de dados se destacam:

1. Exclusão acidental

2. Confusão e lacunas na política de retenção

3. Ameaças internas à segurança

4. Ameaças externas à segurança

5. Requisitos legais e de conformidade

6. Gerenciamento de implantações híbridas de e-mail e migrações para o Microsoft 365

7. Estrutura de dados do Teams

Fonte: 7 etapas para uma estratégia de segurança holística, Microsoft

1. Exclusão acidental

Digamos que você exclua um usuário. Intencionalmente ou não, essa exclusão é replicada em toda a rede, juntamente com a exclusão da conta e da caixa de correio do OneDrive for Business. Sem alternativas, as lixeiras nativas e os históricos de versão do Microsoft 365 são limitados em sua proteção contra perda de dados, o que pode transformar um simples job de backup em um grande problema, depois que o Microsoft 365 tiver excluído com redundância geográfica os dados para sempre ou após o período de retenção terminar.

Existem dois tipos de exclusão na plataforma do Microsoft 365: exclusão reversível e exclusão irreversível. Um exemplo de exclusão reversível é esvaziar a pasta "Itens Excluídos". Também é conhecido como "Excluído permanentemente", embora, nesse caso, o permanente não seja completamente permanente, já que o item ainda pode ser encontrado na pasta "Itens recuperáveis". Uma exclusão irreversível acontece quando um item é marcado para ser limpo completamente do banco de dados da caixa de correio. Depois que isso acontece, o item não pode mais ser recuperado e ponto final. Mas com uma solução de backup à prova de falhas adequada, perder dados por uma exclusão acidental é impossível.

2. Confusão e lacunas na política de retenção

O ritmo acelerado dos negócios na era digital leva a políticas em contínua evolução, incluindo políticas de retenção que são difíceis de acompanhar e ainda mais de gerenciar. Assim como a exclusão reversível e irreversível, o Microsoft 365 tem políticas limitadas de retenção e backup que só conseguem lidar com a perda conjuntural de dados — e não podem ser consideradas uma solução de backup totalmente abrangente.

Outro tipo de recuperação, uma restauração pontual de itens de caixa de correio, não está no escopo de uma licença padrão do Microsoft 365. Em caso de problema catastrófico, uma solução de backup pode oferecer a capacidade de reverter a um momento no tempo anterior ao problema e "salvar o dia". Além disso, com uma solução de backup feita especificamente para o Microsoft 365, não há lacunas na política de retenção nem inflexibilidades na restauração. Backups de curto prazo ou arquivos de longo prazo, restaurações granulares ou de um momento no tempo - tudo está sempre ao seu alcance, tornando a recuperação de dados rápida, fácil e confiável.

3. Ameaças internas à segurança

A ideia de uma ameaça à segurança traz à mente hackers e vírus. No entanto, as empresas sofrem com ameaças internas, que acontecem com mais frequência do que você imagina. As organizações acabam vítimas de ameaças causadas por seus próprios funcionários, de modo intencional ou não. O acesso a arquivos e contatos muda com tanta rapidez que pode ser difícil ficar de olho naqueles em quem você depositou a maior confiança.

A Microsoft não tem como saber a diferença entre um usuário normal e um funcionário demitido que tenta excluir dados essenciais da empresa antes de sair da empresa. Além disso, alguns usuários criam, inadvertidamente, ameaças graves ao fazer o download de arquivos infectados ou ao vazar acidentalmente nomes de usuário e senhas para sites que acreditavam ser confiáveis. Outro exemplo grave é a falsificação de evidências. Imagine um funcionário excluindo estrategicamente e-mails ou arquivos, deixando esses objetos fora do alcance dos departamentos jurídico, de conformidade ou de RH. Quando seus dados do Microsoft 365 estão devidamente protegidos, em local externo e na nuvem, camadas de proteção são adicionadas para combater essas ameaças internas, garantindo que seus dados permaneçam seguros e recuperáveis.

4. Ameaças externas à segurança

Depois, é claro, há ameaças maliciosas externas. Malware e vírus, como o ransomware, causaram danos graves a organizações de todo o planeta. Além do risco à reputação da empresa, isso ameaça também a privacidade e a segurança dos dados internos e de clientes.

Ameaças externas costumam se infiltrar facilmente por meio de e-mails e anexos. Nem sempre é suficiente educar os usuários sobre o que procurar, especialmente quando as mensagens infectadas parecem tão atraentes. As funções limitadas de backup e recuperação do Exchange Online são inadequadas para lidar com ataques graves. Backups regulares, principalmente aqueles gerenciados externamente e na nuvem por meio de um serviço de backup, garantem que uma cópia separada de seus dados não esteja infectada e seja rapidamente recuperável, superando drasticamente as funções limitadas de backup e recuperação do Exchange Online. Além disso, as principais soluções de serviço de backup se integraram ao Microsoft 365 Backup Storage, tornando realidade para as organizações a recuperação rápida de ransomware de grandes conjuntos de dados.

5. Requisitos legais e de conformidade

Às vezes, você precisa recuperar inesperadamente e-mails, arquivos ou outros tipos de dados em meio a uma ação legal. Algo que você nunca acha que vai acontecer com você até que aconteça. O Microsoft 365 inclui algumas redes de segurança (retenção de litígio e retenção), integradas ao software, mas elas estão longe de ser uma solução de backup robusta e não manterão sua empresa livre de problemas jurídicos.

Com um serviço de backup confiável, se você excluir acidentalmente e-mails ou documentos antes de implementar uma retenção legal, ainda poderá recuperá-los e garantir o cumprimento de suas obrigações legais. Os requisitos legais, requisitos de conformidade e regulamentos de acesso variam de acordo com o setor e o país, mas multas, penalidades e disputas legais são três coisas que sua lista de tarefas gostaria de não ter.

Melhor ainda, se você não sabe por onde começar, já que muitos de nós simplesmente não temos capacidade para acompanhar as mudanças na legislação, nas regulamentações e nos requisitos, um serviço de backup cuidará disso para você. Com recursos de monitoramento e relatórios que ajudam a cumprir os requisitos normativos e de conformidade, e com a velocidade e a facilidade que as implantações de serviços de backup são capazes, a tranquilidade de que você está atendendo a esses requisitos pode ser obtida em questão de minutos.

6. Gerenciamento de implantações híbridas de e-mail e migrações para o Microsoft 365

As organizações que adotam o Microsoft 365 geralmente precisam de uma janela transitória entre o Exchange no local e o Microsoft 365 Exchange Online. Essa configuração, em que parte do sistema de e-mail permanece no local enquanto o restante é movido para o Microsoft 365 Exchange Online, pode oferecer mais flexibilidade e controle, o que é de fato comum. Porém, por sua vez, introduz complexidades adicionais de gerenciamento, especialmente em relação aos backups. O gerenciamento de múltiplos ambientes requer uma supervisão cuidadosa para que os dados fluam perfeitamente e sejam protegidos.

É aqui que um serviço de backup para o Microsoft 365 se torna inestimável. O serviço de backup certo da Microsoft lida com implantações híbridas de e-mail de forma eficiente, tratando da mesma forma os dados do Exchange em sistemas locais e do Microsoft 365. Isso torna o local de origem irrelevante, simplifica o processo de backup e elimina a necessidade de gerenciar vários sistemas separados.

7. Estrutura de dados do Teams

Mais do que nunca, as pessoas estão criando equipes para colaboração, projetos e iniciativas especiais, tudo em um ritmo cada vez mais rápido. Mas depois de concluir um projeto, é importante manter uma cópia dele para necessidades de longo prazo, como solicitações legais e de conformidade. É nesse ponto que as organizações geralmente encontram problemas. Mais vezes do que você gostaria, esses Teams são excluídos por engano ou a retenção é mal aplicada e, ao fazer isso, tornam arquivos e documentos essenciais indisponíveis.

Com um serviço de backup do Microsoft 365, esse nunca é o caso. Seus dados estão sempre lá, não importa quem os exclua ou o que os exclua. Pode até ajudar em cenários de curto prazo. Por exemplo, se um funcionário diz algo inapropriado em uma conversa do Teams e exclui a mensagem, os backups são fáceis de acessar. Os dados do Teams estão sempre a apenas alguns cliques de serem recuperados e disponíveis ao departamento de RH para análise.

Mais do que tudo, é fundamental confiar nos seus backups. Saber que eles existem e estão protegidos adequadamente oferece proteção contra o desconhecido, mas também oferece várias formas de restaurar Teams ou canais perdidos ou acidentalmente excluídos. Adotar um serviço de backup desenvolvido especialmente para o Microsoft Teams garante que seus dados estejam sempre disponíveis, não importa o que aconteça ou quando.

Motivo bônus: Gerenciamento de acesso e identificação

O Entra ID (antigo Azure Active Directory) funciona como a base do Microsoft 365, integrando os serviços de gerenciamento de identidade e acesso. Ele é responsável por fornecer contas de usuários e grupos, garantindo que eles possam acessar apenas os recursos para os quais têm permissão. Sua importância não pode ser exagerada, e é por isso que os agentes de ameaças reconhecem que a maneira mais rápida de colocar uma organização de joelhos é atacando o Entra ID, com ataques que aumentam para 600 milhões todos os dias.

A necessidade de proteger o Entra ID vai além das ameaças de cibersegurança, os desafios que as organizações enfrentam são os encontrados nas seções anteriores — requisitos complexos de conformidade, limites de lixeira, exclusões acidentais e configurações incorretas de políticas. A segurança da identidade da sua empresa é, no fim das contas, sua responsabilidade. Uma parte importante da proteção dos dados do Microsoft 365 é garantir uma proteção abrangente para os usuários, grupos, registros de aplicações e outros objetos relacionados do Entra ID.

Fonte: Relatório de Defesa Digital da Microsoft 2024

Conclusão

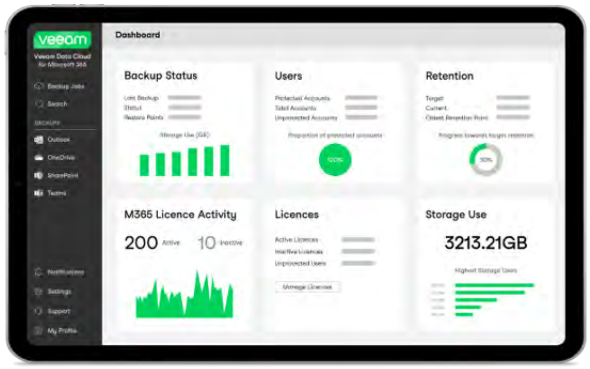
Reserve um momento para avaliar sua postura de segurança atual. Pode haver lacunas que você não sabia que existiam. Você já tomou uma decisão inteligente ao implantar o Microsoft 365. Agora, combine-o com um serviço de backup que forneça acesso e controle completos sobre os seus dados e evite riscos desnecessários de perda de dados.

Você não precisa mais investir tempo, dinheiro e recursos associados a uma solução de software. Com o **Veeam Data Cloud *for Microsoft 365***, você pode utilizar um serviço completo com storage ilimitado incluído, e escolher entre um dos três planos para cumprir seus objetivos de backup e recuperação de desastres. Quer você precise de velocidade e escala de backup e recuperação, controle e flexibilidade ou de uma combinação de ambos, a Veeam fez uma parceria com a Microsoft para garantir que seus dados estejam sempre protegidos, recuperáveis e escaláveis paraas necessidades do seu negócio.

Se você achou esse relatório útil, recomendamos que você o envie por e-mail para um colega: Encaminhe este relatório.

Veeam Data Cloud *for Microsoft 365*:

A proteção de dados resiliente ficou mais simples



- Tecnologia de backup confiável e líder do setor para Microsoft 365
- Serviço de backup com tudo incluso, com storage ilimitado
- Com o novo Microsoft 365 Backup Storage

→ Solicite demonstração

→ Entre em contato conosco

→ **Tem interesse na proteção do Entra ID? Leia o white paper *6 motivos para fazer backup do Microsoft Entra ID*.**