Os 7 motivos críticos para fazer backup do Office 365

Por que as organizações
precisam proteger os dados do Office 365?

VEEAM

TECH VIEW

Introdução

Você tem o controle dos seus dados do Office 365? Você tem acesso a todos os itens dos quais precisa? A reação instantânea normalmente é "claro que sim" ou "a Microsoft toma conta disso tudo".

Mas parando para pensar, você tem certeza?

A Microsoft toma conta de grande parte desse aspecto, além de oferecer um ótimo serviço aos seus clientes. No entanto, o foco principal da Microsoft é gerenciar a infraestrutura do Office 365 e manter o tempo de atividade para os seus usuários. Ela delega a VOCÊ a responsabilidade sobre os seus dados. O equívoco em achar que a Microsoft faz o backup completo dos seus dados por você é bastante comum. Sem uma mudança de pensamento, pode haver consequências desastrosas, caso essa responsabilidade não receba a devida atenção.

No fim das contas, você precisa ter garantidos o acesso e o controle sobre seus dados do Exchange Online, SharePoint Online, OneDrive for Business e Microsoft Teams.

Esse relatório explora os perigos de não ter um backup do Office 365 em seu arsenal e por que as soluções de backup para Microsoft Office 365 preenchem a lacuna da proteção de dados e da retenção em longo prazo.

"Nós nos preocupávamos com as políticas de retenção e backup do Office 365. Foi por isso que decidimos garantir que tivéssemos um backup dos nossos dados que residem no Office 365."

— **Karen St.Clair,** Gerente de TI, Columbia Power & Water Systems

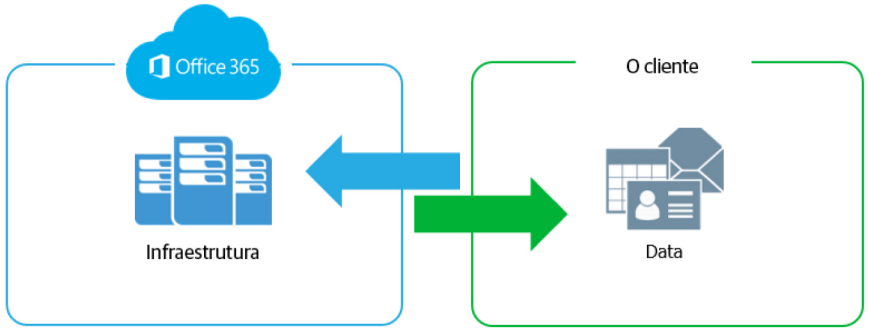
O grande equívoco sobre o Office 365

O engano se dá entre a percepção da responsabilidade da Microsoft e a realidade da responsabilidade do usuário quanto à proteção e retenção em longo prazo dos seus dados do Office 365. Muitas vezes, há diferença entre o que a Microsoft oferece em relação a backup e capacidade de recuperação e o que os usuários presumem receber. Ou seja, além das precauções padrão de que o Office 365 dispõe, talvez você precise reavaliar o nível de controle que tem sobre seus dados e quanto acesso realmente tem a eles.

O Microsoft Office 365 oferece redundância geográfica, que costuma ser confundida com um backup. Um backup acontece quando uma cópia histórica dos dados é feita e então armazenada em outro local. No entanto, é ainda mais importante que você tenha acesso direto e controle sobre esse backup. Assim sendo, em caso de perda de dados, exclusão acidental ou ataque intencional, você pode se recuperar rapidamente. A redundância geográfica, por outro lado, 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.

Fonte: https://docs.microsoft.com/en-us/azure/security/fundamentals/shared-responsibility

A Microsoft se encarrega da infraestrutura, mas os dados continuam sendo responsabilidade do cliente



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

— Documentação da Microsoft

Os 7 motivos pelos quais é essencial fazer backup do Office 365

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

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 da demora entre o comprometimento dos dados e sua descoberta é de mais de 140 dias [1]. Essa lacuna chega a ser chocante de tão grande. É alta a probabilidade de você não notar que alguma coisa está faltando ou foi perdida, até que seja tarde demais para a lixeira resolver.

Em conversas com centenas de profissionais de TI de todo o planeta, que migraram para o Office 365, sete vulnerabilidades na proteção de dados se destacam:

Exclusão acidental

Confusão e lacunas na política de retenção

Ameaças internas de segurança

Ameaças externas de segurança

Requisitos legais e de conformidade

Gerenciamento de implantações híbridas de e-mail e migrações para o Office 365

Estrutura de dados do Teams

[1] http://info.microsoft.com/rs/157-GQE-382/images/EN-GB-CNTNT-eBook-Security-HolisticVision.pdf

1 Exclusão acidental

Se você excluir um usuário, intencionalmente ou não, essa exclusão é replicada em toda a rede, juntamente com a exclusão da conta e da caixa de correio desse usuário no OneDrive for Business.

As lixeiras nativas e os históricos de versão incluídos no Office 365 são limitados em sua proteção contra perda de dados, o que pode transformar uma recuperação simples de um backup adequado em um grande problema, depois que o Office 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 Office 365: a temporária ou reversível e a irreversível. Um exemplo de exclusão reversível é esvaziar a pasta Itens Excluídos. Isso também é conhecido como "exclusão permanente". Neste caso, ela não é completamente permanente, já que o item ainda pode ser encontrado na caixa de correio 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.

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 as exclusões reversível e irreversível, o Office 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, a dos itens de caixa de correio a um momento no tempo, não está no escopo da Microsoft. 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".

Com uma solução de backup para o Office 365, não há lacunas na política de retenção nem inflexibilidade na restauração. Backups de curto prazo ou arquivos de longo prazo, restaurações granulares ou de um momento no tempo, tudo está acessível para tornar a recuperação de dados rápida, fácil e confiável.

3
Ameaças internas de segurança

A ideia de uma ameaça de 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 é a falsificação de evidências. Imagine um funcionário excluindo estrategicamente e-mails ou arquivos, deixando esses objetos fora do alcance do departamento jurídico, de conformidade ou de RH.

4
Ameaças externas de segurança

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

Ameaças externas podem se infiltrar por meio de e-mails e anexos, e nem sempre basta instruir os usuários nos cuidados a se tomar – especialmente quando as mensagens infectadas são tão atraentes e convincentes. As funções limitadas de backup/recuperação do Exchange Online são inadequadas para lidar com ameaças graves. Backups frequentes ajudam a manter uma cópia separada e não infectada de seus dados, com a qual você pode se recuperar rapidamente.

5
Requisitos legais e de conformidade

Às vezes, é preciso recuperar inesperadamente e-mails, arquivos ou outros tipos de dados em meio a um processo judicial. Algo que você nunca acha que vai acontecer, até o dia em que acontece. A Microsoft integrou algumas redes de segurança (retenção de litígio e retenção). Mas elas não são uma solução de backup robusta, capaz de manter sua empresa livre de problemas jurídicos. Por exemplo, com uma solução de backup, se você excluir acidentalmente e-mails ou documentos antes de implementar uma retenção de litígio, ainda poderá recuperá-los e garantir o cumprimento de suas obrigações legais.

Os requisitos legais, requisitos de conformidade e regulamentações de acesso, variam de acordo com o setor e o país, mas as multas, penalidades e disputas legais são três problemas que você não quer ter na sua lista de afazeres.

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

Organizações que adotam o Office 365, normalmente precisam de uma janela de tempo para a transição entre o Exchange local e o Office 365 Exchange Online. Alguns ainda deixam uma pequena parte do sistema legado instalada para ter mais flexibilidade e controle. Essas implantações híbridas de e-mail são comuns, mas ainda assim apresentam desafios adicionais de gerenciamento.

A solução de backup certa para o Office 365 deve ser capaz de lidar com implantações híbridas de e-mail, além de tratar da mesma forma os dados do Exchange, tornando seu local de origem irrelevante.

Além disso, você deve ser capaz de armazenar os dados em qualquer lugar que escolher, seja no local, em storage de objeto na nuvem, como o AWS S3 ou Blob do Azure, ou com um provedor de serviços gerenciados.

7 Estrutura de dados do Teams

Com o aumento do trabalho remoto, o Microsoft Teams está ganhando ampla adoção. Agora, ele é o centro do nosso universo de produtividade. A Microsoft estrutura o Teams como uma interface de usuário que reúne serviços do Office 365, como o SharePoint Online e o OneDrive for Business. Essa abordagem fornece uma comunicação em tempo real e colaboração ágil para as equipes.

Você precisa proteger os dados nesses locais, mas não apenas isso. O Teams tem configurações e associações. Todos eles precisam ser protegidos e permanecer recuperáveis. Uma solução desenvolvida especificamente para backup pode proteger não só os dados, mas também essas configurações e as interconexões associadas entre as aplicações.

Mais do que nunca, as pessoas estão usando o Teams para projetos e iniciativas especiais, em um ritmo acelerado. Porém, após concluir um projeto, você provavelmente precisa manter uma cópia dele para necessidades de longo prazo, como solicitações legais e de conformidade. O que ocorre muitas vezes, é que esses Teams são excluídos por engano ou a retenção é mal aplicada, o que torna outros arquivos ou documentos essenciais indisponíveis.

Os backups também podem ajudar em cenários de curto prazo. Por exemplo, se um funcionário diz algo inapropriado em uma conversa do Teams e depois exclui a mensagem, ter um backup tornaria possível recuperar a conversa e disponibilizá-la ao departamento de RH para análise. Fornecedores de backup terceirizados não só oferecem proteção contra o desconhecido como também podem oferecer várias formas de restaurar equipes ou canais perdidos ou acidentalmente excluídos.

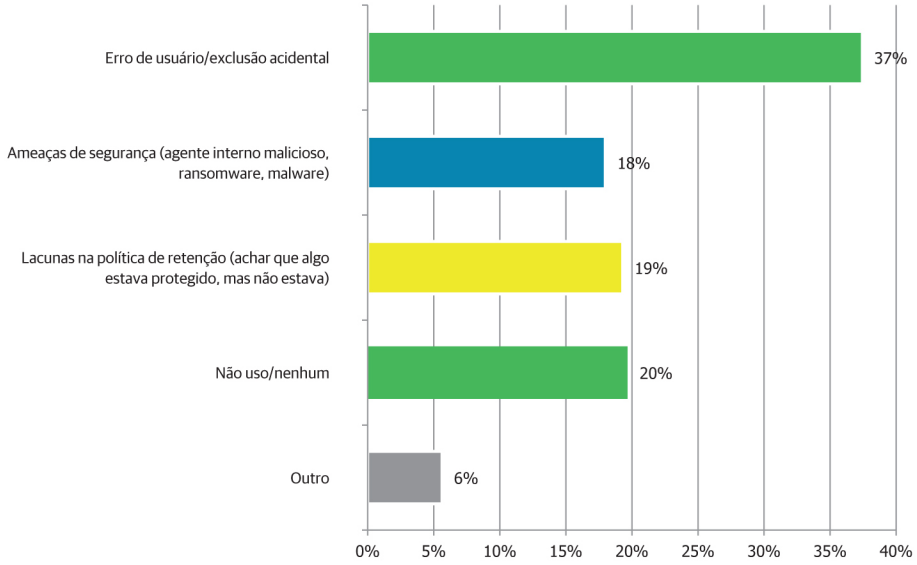
Com que frequência esses motivos acontecem?

Agora você sabe por que é crucialmente importante fazer o backup dos seus dados do Office 365. Mas você deve estar se perguntando até que ponto essas sete vulnerabilidades de proteção de dados ocorrem de fato. Infelizmente, a resposta é que ocorrem com frequência excessiva...

Mais de 1.000 profissionais de TI foram consultados sobre as formas de perda de dados que experimentaram na nuvem. A lista inclui erro de usuário/exclusão acidental, ameaças de segurança e lacunas de retenção, indo de 18% a 37%[2].

A realidade assustadora é que apesar de dados sigilosos na nuvem serem armazenados em documentos do Office, estima-se que 76% deles não são incluídos no backup[2]. De fato, o IDC diz que 6 de cada 10 empresas não têm um plano de proteção de dados para seus ativos do Office 365[3]. Você trabalha em uma dessas empresas desprotegidas? Se sim, agora você já tem o conhecimento oferecido nesse relatório para incentivar sua empresa a proteger seus dados do Office 365.

P14. Que tipos de perda de dados você já sofreu na nuvem? (Marque todas as opções que se aplicam)



Entrevistados = 1.579

[2]Pesquisa da Veeam com clientes, setembro de 2019
[3]IDC: Por que uma estratégia de backup para o Microsoft Office 365 é essencial, 2019

Conclusão

Vá em frente e olhe com mais atenção. Há lacunas de segurança que você pode não ter notado antes.

Você já tomou uma decisão de negócios inteligente ao implantar o Microsoft Office 365, agora encontre uma solução de backup que ofereça a você acesso e controle completos dos seus dados do Office 365 e evite riscos desnecessários de perda de dados.

Se achou esse relatório útil, incentivamos você a enviá-lo por e-mail a um colega:
Encaminhar este relatório

Saiba mais sobre o backup do Office 365 em:
https://www.techview.com.br/

About Techview Informática