Erisvan Barboza

Matheus Martins

Fabíola Braga

**Estratégias para aplicação dos Backups em empresas**

1. **Backup Completo:**

* Realize um backup completo inicial de todos os dados da empresa, incluindo sistemas, aplicativos, bancos de dados e arquivos importantes. Geralmente utilizamos esse backup para implantações e grandes volumes de dados.
* Agende backups completos regulares, dependendo da quantidade de dados e das mudanças ocorridas. Geralmente, backups completos semanais são uma boa prática.

1. **Backup Incremental:**

* Copia apenas os dados que foram alterados ou adicionados desde o último backup, seja ele completo ou incremental.
* É mais rápido e requer menos espaço de armazenamento em comparação com o backup completo.
* A restauração pode ser mais demorada, pois é necessário recuperar o último backup completo e todos os backups incrementais subsequentes até o momento desejado de restauração.
* Ideal para ambientes com muitas alterações diárias, pois economiza tempo e espaço.

1. **Backup Diferencial:**

* Copia apenas os dados que foram alterados desde o último backup completo, não importando se foram feitos backups incrementais desde então.
* Pode levar mais tempo para ser concluído em comparação com o backup incremental, pois copia mais dados a cada vez.
* A restauração é mais rápida do que com o backup incremental, pois é necessário recuperar apenas o último backup diferencial e o backup completo original.
* É mais adequado para ambientes com poucas mudanças diárias ou com limitações de tempo de backup, pois cada backup diferencial pode ser maior do que o incremental.

**Mídias de armazenamento**

**Discos rígidos (HDD):** São dispositivos de armazenamento magnético que utilizam discos rotativos para armazenar dados. São amplamente utilizados devido à sua capacidade de armazenamento, custo acessível e velocidade de leitura/gravação. Podem ser internos (instalados diretamente no computador) ou externos (conectados através de portas USB, Thunderbolt, etc.).

**Servidores de rede (NAS - Network-Attached Storage):** Os servidores NAS são dispositivos dedicados ao armazenamento em rede. Permitem o compartilhamento e o armazenamento centralizado de dados em uma rede local. São úteis para empresas com várias estações de trabalho que precisam de acesso compartilhado e seguro aos dados.

**Armazenamento em nuvem:** O armazenamento em nuvem é uma opção cada vez mais popular, na qual os dados são armazenados em servidores remotos e acessados pela internet. Oferece escalabilidade, flexibilidade e acessibilidade de qualquer lugar. Os dados são armazenados em data centers gerenciados por provedores de serviços em nuvem.

**A importância do Armazenamento off-site**

O armazenamento off-site é fundamental para proteger os dados em caso de desastres físicos, como incêndios, inundações ou roubo. Envolve a cópia dos backups para uma localização geograficamente separada da empresa. Pode ser um centro de dados externo, outra filial da empresa ou um serviço de armazenamento em nuvem. O armazenamento off-site garante a recuperação dos dados mesmo em situações em que o local principal da empresa seja comprometido.

**A importância de testar documentar a estratégia de backup e da conformidade e regulamentações**

É crucial testar regularmente a estratégia de backup para garantir que os backups estão sendo realizados corretamente e que os dados podem ser restaurados com sucesso. Além disso, é importante documentar a estratégia de backup, incluindo os procedimentos de backup, os horários e a retenção dos backups. Isso ajuda a garantir a consistência e a eficácia da estratégia.

Empresas devem considerar os requisitos de conformidade e regulamentações aplicáveis aos seus setores, como o GDPR (Regulamento Geral de Proteção de Dados) na União Europeia ou a Lei Geral de Proteção de Dados (LGPD) no Brasil. É importante garantir que a estratégia de backup esteja em conformidade com essas regulamentações, incluindo medidas de segurança adequadas para proteger os dados pessoais.

**O que é o Kali Linux**

O Kali Linux é uma distribuição Linux especializada voltada para testes de segurança, análise de vulnerabilidades e realização de testes de penetração (pentest). Ele foi desenvolvido pela Offensive Security com o objetivo de fornecer uma plataforma completa e poderosa para profissionais de segurança cibernética, pesquisadores e entusiastas do hacking ético.

O sistema operacional é baseado no Debian e inclui uma ampla variedade de ferramentas de segurança e hacking pré-instaladas, permitindo que os usuários realizem testes em redes, sistemas e aplicativos para identificar e corrigir possíveis falhas de segurança. Essas ferramentas são organizadas de maneira intuitiva para facilitar a utilização e o acesso rápido.

O Kali Linux é amplamente utilizado por profissionais de segurança cibernética para avaliar a postura de segurança de sistemas e redes, ajudando a proteger e melhorar a segurança em ambientes corporativos e outros contextos. No entanto, é importante observar que, por ser uma ferramenta poderosa, seu uso deve ser feito com responsabilidade e de acordo com as leis e regulamentos locais.

* Melhores práticas de segurança para poder usar o Kali Linux em uma máquina virtual
* Senhas fortes: Use senhas difíceis de adivinhar.
* Atualizações regulares: Mantenha o Kali Linux sempre atualizado.
* Firewall: Configure um firewall para bloquear acessos indesejados.
* Remova software desnecessário: Desinstale programas que não precisa.
* Não use em ambiente de trabalho: Use o Kali Linux apenas para testes de segurança.
* Criptografia: Proteja informações importantes com criptografia.
* Controle de acesso: Limite o acesso à máquina virtual.
* Registre atividades: Verifique registros para encontrar atividades suspeitas.
* Faça backup: Faça cópias de segurança dos seus dados importantes.
* Proteção contra vírus: Use ferramentas de proteção contra vírus.
* Rede isolada: Coloque o Kali Linux em uma rede separada, se possível.
* Remova configurações inseguras: Desligue configurações inseguras.
* Baixe de fontes confiáveis: Obtenha software apenas de lugares confiáveis.
* Use ambientes isolados: Isole processos para evitar problemas.