

O BACKUP QUE PODE SALVAR SUA EMPRESA

Alexandre Ayres | Neocom

27/08/2021

A maior parte das pessoas já passou por alguma situação, seja na sua vida pessoal ou profissional, em que foi confrontada com a pergunta: você tem backup destes dados?

O backup é uma cópia de segurança de qualquer tipo de dado, registro, arquivo, aplicação, sistema operacional ou ambiente que você utilize. A existência de um backup bem feito pode te salvar de graves problemas e, em tempos de ransomware, pode salvar o seu negócio.

Ransomware é um malware que pode bloquear dados de computadores e servidores por meio do uso de criptografia. É literalmente um sequestro de dados! O modus operandi pode variar, mas, no geral, esse malware é inserido em sua rede de computadores por meio de uma invasão e usado para exigir dinheiro da empresa, em troca dos códigos que permitem a descryptografia.

Esse é o ponto importante: em uma invasão de ransomware os dados não são roubados, extraídos ou copiados. Eles são apenas criptografados e se tornam inúteis. Apesar de ser uma situação complexa e trabalhosa, a solução mais viável para esse tipo de situação é, simplesmente, a recuperação de dados por meio da restauração do backup.

Isso pode significar muito mais do que uma redução de danos: em um ataque ransomware o backup de dados pode significar a sobrevivência do seu negócio.

O backup pode parecer uma atividade básica e a maior parte dos gestores de concessionárias de veículos provavelmente acredita que isso está resolvido em sua empresa. Porém, problemas nas rotinas e estruturas de backup são muito mais comuns que se imagina.

Você pode afirmar que sua empresa realmente tem backup de dados?

Se você não tem segurança para responder positivamente a essa pergunta, seguem cinco dicas para implantar ou aperfeiçoar os processos de backup da sua empresa:

DICA NÚMERO 1: DEFINA QUAL A MELHOR SOLUÇÃO DE BACKUP PARA SUA EMPRESA

Existem inúmeras soluções de backup e é fundamental decidir qual é a melhor para a sua empresa. Na prática, essa decisão vai depender de fatores como a sua atividade, o tamanho da sua empresa, os sistemas e aplicações que você usa e até questões e exigências legais.

Seguem algumas perguntas que podem lhe ajudar nessa definição:

- A solução de backup deve abranger quais dados, sistemas ou ambientes?
- Qual é a volumetria desses dados e registros?
- Com que frequência o backup deve ser realizado?
- Por quanto tempo o backup deve ser mantido?

DICA NÚMERO 2: REDUZA O VOLUME DO SEU BACKUP

A duplicação de dados consiste em identificar, analisar e remover duplicidades, com o objetivo de enxugar a quantidade de dados a ser armazenada. Com essa medida, reduz-se o volume de dados que precisam ser gerenciados e protegidos, permitindo um nível superior de visibilidade e segurança.

DICA NÚMERO 3: ARMAZENE SEU BACKUP EM LOCAL SEGURO

Após organizar os dados e produzir as cópias, é necessário armazená-las em uma local seguro e criptografado, para mantê-las afastadas dos ataques. Essa, inclusive, é uma exigência da Lei Geral de Proteção de Dados (LGPD).

As principais opções são os discos rígidos externos, as opções em fita e o backup em nuvem. A melhor prática neste caso é optar por salvar os seus dados em mais de um local. Atualmente, grande parte das empresas mantém, ao mesmo tempo, um backup físico (no seu próprio ambiente) e outro em nuvem (Google Cloud, AWS, Azure ou outras).

DICA NÚMERO 4: REALIZE BACKUPS PERIODICAMENTE E FAÇA VERSIONAMENTOS

A periodicidade de execução do backup depende da atividade da sua empresa e criticidade dos dados a serem armazenados. Discuta com sua equipe quantas vezes por dia ou semana se deve fazer um backup, de acordo com suas necessidades.

Versionar o backup também é uma boa prática. Com isso você não exclui o backup anterior e cria assim uma “cadeia de memória” das suas informações. Caso algo dê errado com o backup de hoje, você ainda assim vai poder buscar informações em arquivos de backups antigos para restaurar seus dados perdidos.

DICA NÚMERO 5: TESTE SEUS BACKUPS

Então você criou todos os seus backups seguindo as melhores práticas para isso e aconteceu o inesperado. Você precisou restaurar dados! Mas quando buscou o backup para restauração, descobriu que houve alguma falha de processo ou estrutura e os dados não estavam disponíveis. Infelizmente essa não é uma surpresa incomum... Testar manualmente todos os seus backups faz parte de uma rotina bem planejada, afinal você não pode esperar o prejuízo acontecer para agir.

Alexandre Ayres é Professor na Fundação Getúlio Vargas e Diretor da Neocom Informação Aplicada, empresa especializada em geração de inteligência para o mercado automotivo.

Conheça mais sobre a Neocom no site www.neocom.info.