

É muito importante entender a necessidade de proteger os dados, aplicativos e sistemas das empresas. Ano após ano aumentam os ataques informáticos e a segurança no ciberespaço se transforma em uma prioridade para todas as organizações. O backup é o primeiro nível na proteção de dados, mas não é suficiente.

Daniela Costa, VP para a América Latina da Arcserve, afirma que estamos em um mundo muito competitivo, no qual as empresas precisam ser cada vez mais produtivas. E destaca que é necessário reduzir ou eliminar riscos de indisponibilidade, bem como impactos financeiros negativos associados, que possam afetar a produtividade da equipe de trabalho e do negócio de uma empresa.

Crer que a empresa está 100% protegida

Há grandes organizações governamentais, financeiras e tecnológicas, que sofreram ataques cibernéticos, o que demonstra que apesar dos altos orçamentos e sistemas de segurança complexos, nada garante a segurança. Por esse motivo, é importante entender que se trata de um processo de investimento e evolução constantes.

Crer que com apenas uma solução implementada se está 100% protegido e não complementar as ferramentas de segurança com processos documentados e equipe treinada

É importante verificar que as soluções implementadas se complementem e que sejam as mais completas possíveis, que os processos de segurança da empresa, em geral, estejam conectados e que tudo esteja documentado e definido de comum acordo com todas as equipes envolvidas. Contar apenas com soluções pontuais sem um contexto de todo o ambiente pode gerar riscos desnecessários e possíveis falhas caso ocorra um desastre.

Trabalhar com as probabilidades de que possa ocorrer um desastre

A pergunta importante que deve ser feita não é se, mas sim quando um desastre acontecerá. A perda de dados pode ocorrer por vários motivos, dos mais simples aos mais complexos: erros humanos, problemas com ar condicionado nos escritórios, falha de hardware e perda de energia (apagões) são desastres muito comuns enfrentados por qualquer empresa.

Não assumir que o importante não é só fazer o backup

As empresas devem assumir que as ameaças evoluem. O modo como elas agem e como podem antecipar-se a elas fará como que o monitoramento seja realmente eficaz.

Atualmente, falamos de recuperação completa, de continuidade dos negócios e não apenas de backup. Garantir a recuperação total de todos os sistemas críticos no menor tempo possível é essencial para manter-se competitivo nos dias de hoje.

Segundo uma pesquisa recente da Arcserve, para seus clientes na América Latina, apenas 37% das empresas têm um plano completo de recuperação de desastres documentado e a metade deles jamais fez testes para verificar se o plano funcionava ou não.

Não assumir que a continuidade dos negócios é uma das prioridades no orçamento de TI

50% dos clientes da Arcserve disseram não saber calcular o custo de um desastre; fato que afeta diretamente a rentabilidade das empresas. Esses custos podem ser diretos – custo para subir todo o ambiente em caso de desastre: substituição de hardware, custo de funcionários/hora, downtime de sistemas críticos como faturamento -, mas também custos indiretos associados à imagem perante clientes e reputação da empresa em seu segmento.

Apenas 9% das empresas expressaram que o custo associado a um evento de perda de dados em suas empresas é igual ou maior que US\$ 50.000.

É importante observar que a preocupação sobre a segurança e disponibilidade da informação e sistemas é uma realidade atual da área de TI. Em relação a esse problema, a Arcserve lançou em fevereiro de 2016 a versão 6 da sua solução, Unified Data Protection, dirigida ao setor corporativo, que combina tecnologias de backup, replicação e alta disponibilidade para ambientes multiplataforma Windows e Linux, virtuais, físicos e na nuvem. Além disso, conta com uma interface simples e amigável que também facilita a implementação e gerenciamento por parte do administrador, sem altos custos adicionais de manutenção.

Fonte: [Risk Report](#), em 06.05.2016.