Não é de hoje que a segurança é o centro das atenções (e preocupações) no mundo da tecnologia da informação. Mas cada vez mais nos deparamos com notícias de vazamentos de dados, ataques hackers, dentre outros casos de vulnerabilidades em grandes empresas do mundo. Quem não se lembra daquele mega vazamento de informações de 223 milhões de brasileiros em 2021? Desde então foram inúmeros casos conhecidos de negócios que sofreram do mesmo problema.

Outro acontecimento que merece a atenção das empresas na área da segurança da informação é a implementação da Lei Geral de Proteção de Dados (LGPD), pois com ela, as pessoas e empresas necessitam de um cuidado maior no trato das informações de pessoas físicas, como seus clientes, fornecedores e até colaboradores, mas também de outros dados que possam ter sido compartilhados.

Mas a pergunta que fica é: como posso deixar meu sistema protegido?

Primeiro ponto importante saber é que não existe 100% de proteção, segurança da informação e seus métodos sempre busca chegar o mais próximo da segurança total. Um ponto que costumo ouvir é a associação do uso de nuvem às falhas de incidente, minha percepção é que na verdade o aumento nos incidentes são uma consequência no aumento do uso tecnologias em nosso dia a dia, por meio de Cloud Compute. Cloud na verdade permite termos uma estrutura tecnológica mais segura, por vários motivos, mas entre eles o acesso para empresas de todos os tamanhos a tecnologias que antes eram disponíveis apenas para grandes corporações, ou até que não existiam.

Nela também é possível criar dispositivos de segurança, capazes de mitigar ataques, falhas, erros e vulnerabilidades. Assim prevenindo sua empresa de sofrer como os casos relatados acima. Práticas como por exemplo gerenciar e limitar o acesso de certos tipos de informações em usuários de sua corporação, ou o monitoramento constante de seu sistema, que permite agir de forma rápida e assertiva contra qualquer eventual problema.

Modelo de responsabilidade compartilhada

As provedoras de serviços em nuvem, como a Amazon Web Services e o Microsoft Azure, também implementam o modelo de responsabilidade compartilhada. Um documento que delimita as responsabilidades da plataforma e a de seus usuários. Por exemplo, nesse modelo, a provedora se compromete com a segurança de seus serviços e ferramentas, mas os dados, a rede, e as informações nelas colocadas é de responsabilidade do cliente em utilizar as melhores práticas de segurança em seu ambiente em nuvem.

Com esse modelo, é possível realizar uma verdadeira parceria entre a provedora e seu usuário, uma vez que num ambiente on premises a responsabilidade de gerenciar, realizar a manutenção, bem como o a implementação de práticas de segurança de toda a infraestrutura fica inteiramente sob cuidados da empresa.

Well Architected

As maiores provedoras de serviços em nuvem também oferecem um framework que contém as melhores práticas capazes de se extrair o melhor que a tecnologia pode oferecer. Um dos mais conhecidos e utilizados é o AWS Well Architected Framework, que traz um conjunto de boas práticas em um ambiente em nuvem divididos em seis pilares. E um deles é o de segurança. Dentre os principais tópicos desse pilar estão a confidencialidade, o gerenciamento de acesso e permissão dos usuários e a implementação de controles para detectar eventos incomuns e que são capazes de colocar o sistema da empresa em risco.

Os usuários do Microsoft Azure e do Google Cloud também possuem um framework similar que apresentam as melhores formas de manter suas plataformas altamente produtivas e seguras.

É importante ressaltar que a computação em nuvem não é a grande salvadora que irá deixar seu ambiente totalmente impenetrável contra ataques, ou vazamento de dados. O primeiro passo de se manter um sistema seguro é entender que não existe um sistema 100% protegido, uma vez que todos podem estar sujeitos a uma instabilidade na segurança devido a uma falha humana, por exemplo. Com isso e com o auxílio da computação em nuvem, a equipe de TI de sua empresa pode ter acesso as melhores práticas de segurança capazes de mitigar todos esses erros, bem como trazer para dentro de sua empresa uma verdadeira cultura onde a segurança da informação é determinante para o bom andamento dos negócios.

***Flavio Rescia, Co-Founder & CTO da Darede**

Fonte: Abrapp em Foco, em 15.06.2022.