Por Erick Matheus dos Santos (*)

As organizações estão sentindo o calor e a pressão para inovar e criar maneiras de fazer com que

seus negócios permanecerem relevantes. Para as instituições financeiras, em particular, esta situação é ainda mais presente devido à forte concorrência dos gigantes do setor, bem como as startups "nascidas digitais".

Com o cenário regulatório em constante mudança, equilibrar requisitos regulamentares e de conformidade complexos com esforços para aumentar a eficácia e reduzir custos por meio da transformação digital, exigirá processos de negócios mais inteligentes e que demandam atenção com a segurança da informação.

As inovações permitem o acesso ideal do usuário aos sistemas, garantindo a manutenção das medidas de segurança apropriadas. Para um número crescente de organizações, usuários internos e externos estão acessando sistemas de todo o mundo e de uma variedade de dispositivos. Isso significa que as identidades desses usuários e seus acessos associados, em vez da rede, estão formando o novo limite de segurança em torno da organização.

Essa mudança de paradigma destaca a importância de acertar o gerenciamento de identidade e acesso (IAM), tanto para facilitar os negócios quanto para ficar à frente dos requisitos de auditoria, conformidade e regulamentação. Analisando a **Instrução Normativa nº 001/2001**, temos o Princípio da Segregação de Funções, uma regra de controle interno para evitar falhas ou fraudes na entidade, descentralizando o poder e estabelecendo independência para as funções de execução operacional, custódia física e contabilização da informação. Ela alerta que ninguém deve ter sob sua inteira responsabilidade todas as fases inerentes a uma operação.

A informação tem um ciclo de vida de quatro fases: manuseio, no qual dado é criado e manuseado; transporte, que são os meios para o envio dos dados de um local a outro; armazenagem, onde o dado está guardado/custodiado; e descarte, ou seja, quando se dá o ciclo final à informação.

Analisando estas etapas, um dado pode ser vazado como ato intencional em algumas dessas fases para obter algum ganho ou vantagem e, em um ambiente competitivo, cujas mudanças de processo e tecnologia podem impulsionar a organização a novos patamares ou causar riscos significativos e possíveis impactos negativos, é crucial a adoção de medidas de segurança para que dados não caiam nas mãos de alguém mal-intencionado em qualquer etapa do seu ciclo de vida.

Cabe a adoção de procedimentos de segurança como estratégia de prevenção de ataque cibernético, evitando o vazamento de informações sigilosas das empresas. Portanto, para permanecer relevante e permitir que a empresa tenha sucesso em um cenário em rápida mudança, mantendo uma forte postura de risco e segurança, programas, processos, governança e tecnologia de gerenciamento de identidade e acesso precisam ser alinhados.

Investir em uma equipe capacitada na terceirização deste serviço que seja especializada, com profissionais que tenham domínio do tema e que sejam capacitados para proteger seus dados, deve ser levado em consideração num mundo cada vez mais digital e com empresas ingressando para a cultura Data Driven.

(*) **Erick Matheus dos Santos** é consultor sênior de auditoria interna e assessoria financeira da ICTS Protiviti, empresa especializada em soluções para gestão de riscos, compliance, auditoria interna, investigação, proteção e privacidade de dados.