Prodemge destaca Gestão de Identidade e Acesso no combate a riscos cibernéticos

Sex 28 novembro

O índice Global Cybersecurity Index traz informações importantes em um mundo totalmente conectado: o Brasil é um dos maiores alvos de ataques cibernéticos do mundo e projeta investir R$104,6 bilhões em segurança da área entre 2025 e 2028.

Nas empresas, públicas e privadas, a corrida pró segurança da informação é cada vez mais necessária. Diretor de Operações e Infraestrutura da Companhia de Tecnologia da Informação de Minas Gerais (Prodemge), Cassio Matoso, destaca a importância de um tema fundamental para a segurança e a governança digital, a Gestão de Identidade e Acesso (IAM).

“IAM é o conjunto de processos, políticas e tecnologias que garantem que as pessoas certas tenham o acesso adequado aos recursos corretos, pelo tempo necessário, de forma segura e auditável”, explica.

No contexto da Prodemge e do setor público, a IAM é essencial para proteger dados sensíveis de cidadãos e garantir conformidade com normas como a ISO 27001 e a Lei Geral de Proteção de Dados (LGPD).

“O principal objetivo é assegurar a confidencialidade, integridade e disponibilidade das informações, evitar acessos indevidos e fraudes, além da transparência, rastreabilidade e conformidade legal”, acrescenta.

Ações

Matoso lista ações e tecnologias como pilares do processo, e ressalta a importância da LGPD, como a camada adicional de responsabilidade sobre o tratamento de dados pessoais.

“Na prática, a IAM passou a ser também uma ferramenta de governança de privacidade. Todo acesso a dados pessoais deve ser justificado, registrado e minimizado. O princípio da 'necessidade' é o guia: concedemos acesso apenas ao que é estritamente necessário para o desempenho da função”, detalha.

O diretor também cita a evolução, na Prodemge, para a arquitetura Zero Trust. “Nenhum acesso é implicitamente confiável, mesmo dentro da rede interna. Cada tentativa de acesso deve ser autenticada e autorizada, abordagem ainda mais essencial diante da integração com serviços em nuvem”.

Identidades de máquina

A IAM também deve ser aplicada em usuários não humanos, ou identidades de máquina como

APIs, contêineres e processos automatizados — que representam uma parte crescente do ecossistema digital. São necessários autenticação forte e controle de acesso, por exemplo.

“Falhas na gestão dessas identidades é uma das principais vulnerabilidades exploradas nos ataques cibernéticos”, frisa Matoso.

Mudança cultural

O especialista traz alguns dos desafios mais comuns da aplicação da IAM, como integração com sistemas legados e necessidade de mudança cultural. Ele aponta que a boa gestão de identidade não é apenas um tema técnico, mas organizacional, uma responsabilidade que deve ser compartilhada.

Nesse contexto, investir na capacitação de colaboradores e equipes é um dos passos para fortalecer a segurança da informação nas empresas.

A Prodemge já está na terceira temporada de gamificação Hacker Rangers, programa de conscientização e treinamentos que orienta colaboradores sobre boas práticas de senha, phishing, engenharia social, responsabilidade individual no uso de credenciais, dentre outros temas relevantes.

“A cultura de segurança é o elo mais forte de uma boa estratégia de IAM. Com a iniciativa, o aprendizado ocorre de forma lúdica, com cursos, jogos, ciberatitudes e desafios; e cada atividade conta pontos para o ranking geral. Os três primeiros colocados ganham um dia de folga”, descreve.

Futuro

A tendência, aponta o especialista, é de automação, integração e inteligência. “A adoção de IA para detectar comportamentos anômalos, a interoperabilidade entre órgãos públicos e a consolidação de identidades federadas — como o login unificado Gov.br — são o futuro. O objetivo é simplificar o acesso, aumentar a segurança e melhorar a experiência do usuário/cidadão”.