Por Diego Nunes de Araújo (*)

A cada dia, a segurança cibernética está se tornando mais importante, já que a vida dos cidadãos e dos negócios está ligada ao mundo virtual. Por isso, os termos malware, ciberguerra e brute force attack estão mais frequentes e os especialistas em cibersegurança atuam como se estivessem na linha de frente de um campo de batalha.

E esse cenário deve se intensificar. De acordo com a Statista, plataforma on-line especializada em dados de mercado e consumidores, o custo anual dos crimes cibernéticos vai crescer 40% e atingir

US$ 11,5 trilhões em 2023, ou seja, R$ 59 trilhões.

Logo, é possível imaginar que, neste período, ocorrerá um ataque Zero-Day, ou seja, uma invasão em função de uma vulnerabilidade não conhecida de software que ainda não foi identificada pelo fornecedor ou público. Para efeitos de analogia, imagine que uma fechadura da sua casa está quebrada, mas você não sabe e, até que descubra e conserte, os malfeitores tiram proveito dessa situação. Ocorre o mesmo num ataque Zero-Day. Mas, é possível proteger o ambiente de um evento desse nível e manter os dados íntegros. Para isso, devemos seguir as boas práticas de segurança listadas abaixo:

1. Sempre manter os firmwares, hardwares, softwares e sistemas operacionais atualizados. Os fornecedores estão sempre incluindo correções de segurança recém identificadas em novas versões. Isso garante mais segurança;
2. Utilizar equipamentos de segurança, como firewall e VPN, entre outros, que tem como foco proporcionar a proteção essencial contra ameaças, sempre atualizados e configurados para permitir somente transações necessárias.
3. Conscientizar os colaboradores com treinamentos, palestras e políticas de segurança. Com os bons hábitos, os colaboradores estarão seguros no ambiente on-line, apoiando a organização na proteção de ameaças digitais;
4. Utilizar somente softwares necessários, o que reduzirá as vulnerabilidades e os riscos à rede;
5. Tenha uma rotina de backup do seu ambiente. É importante procurar mantê-lo armazenado em outro local além da empresa, reforçando a segurança em caso de acidentes que o comprometa fisicamente.

Um ataque Zero-Day é um risco enorme para as empresas, causando prejuízos incalculáveis. E hoje, mais do que nunca, é fundamental que as organizações invistam em Segurança da Informação para garantir os princípios básicos de confidencialidade, integridade e disponibilidade de ambientes, bem como para se fortalecerem no mercado.

(*) **Diego Nunes de Araújo** é analista de Segurança da Informação da Protiviti, empresa especializada em soluções para gestão de riscos, compliance, ESG, auditoria interna, investigação, proteção e privacidade de dados.