

Desafios da IA: segurança em foco para proteger dados sensíveis

Com aumento do uso da Inteligência Artificial, estratégias de cibersegurança são cruciais para evitar riscos de vazamento de dados.

O avanço da tecnologia da Inteligência Artificial (IA) tem se tornado uma necessidade incontestável para empresas que buscam se destacar no mercado. No entanto, enquanto a popularidade da IA cresce, é crucial que os benefícios dessa tecnologia não encubram os riscos iminentes de cibersegurança.

Um estudo recente do Itaú Unibanco revela um aumento de 196% nos gastos dos brasileiros com ferramentas pagas de IA nos primeiros meses deste ano, em comparação com 2022. Com o destaque atual para ferramentas como o ChatGPT, é evidente que a IA já é uma realidade palpável.

Porém, a crescente dependência também traz riscos, como evidenciado por um estudo da Cyber Haven, que identificou que 11% das informações compartilhadas com o ChatGPT são confidenciais. Diante disso, é essencial adotar estratégias de cibersegurança eficazes para evitar vazamentos e ameaças.

Novos desafios

O avanço tecnológico traz consigo novas dimensões de oportunidades e desafios. A IA se faz presente em aplicativos cotidianos e soluções corporativas, impulsionando a eficiência e a produtividade. No entanto, a dependência dessa tecnologia também expõe as empresas a ameaças cibernéticas significativas.

O estudo do Itaú Unibanco destaca um aumento substancial nos gastos com ferramentas de IA enfatizando a rápida adoção dessa tecnologia. O ChatGPT, por exemplo, trouxe uma nova experiência prática com IA, mas seu uso também acarreta riscos, especialmente quando informações sensíveis são compartilhadas inadvertidamente.

Confidencialidade em risco?

O dado de que 11% das informações compartilhadas são confidenciais é alarmante, considerando o cenário de ataques cibernéticos em constante evolução. Empresas e indivíduos devem reconhecer a importância da segurança da informação ao utilizar ferramentas de IA. Vazamentos de dados podem levar a consequências desastrosas, comprometendo a reputação das empresas e a confiança dos clientes.

A importância da cibersegurança

Embora os benefícios da IA sejam indiscutíveis, é vital reconhecer e abordar os riscos associados. Três aspectos fundamentais merecem atenção especial:

1-Segurança da informação: à medida que a IA se integra a navegadores, sistemas de e-mail e gerenciamento de documentos, novos riscos de segurança surgem. Compartilhar informações sensíveis e pessoais com assistentes virtuais baseados em IA amplia as oportunidades para ataques cibernéticos;

2-Exposição de dados confidenciais: a busca pela eficiência pode levar a divulgação de informações estratégicas da empresa. O estudo da Cyber Haven revelou que 4% dos usuários já compartilharam informações sensíveis, expondo as organizações a ameaças adicionais;

3-Uso indevido e malicioso: enquanto empresas adotam a IA para otimizar operações, criminosos também a exploram para ataques cibernéticos, desinformação e atividades ilícitas. Prejuízos resultantes de tais ações podem abalar a confiança dos usuários nos serviços da empresa.

Estratégias de proteção

Adotar medidas de proteção é imperativo. Estabelecer procedimentos rigorosos para coleta, uso e descarte de dados é essencial para proteger as informações. A utilização de softwares de proteção, senhas fortes e práticas de backup são medidas básicas que reduzem a vulnerabilidade. A implementação de uma governança de IA garante a ética no uso da tecnologia.

Em última análise, a IA é uma ferramenta poderosa que molda nosso futuro. No entanto, devemos usá-la com responsabilidade, adotando medidas de cibersegurança para garantir que sua evolução seja acompanhada pela proteção necessária.