



Mercado Digital

Patricia Knebel

patricia.knebel@jornaldocomercio.com.br

Confira, diariamente, no blog Mercado Digital, conteúdos sobre tecnologia e inovação. Para acessar, aponte a câmera do seu celular para o QR Code.

jornaldocomercio.com/mercadodigital



IA também pode ser alvo de sérios ataques

Embora a Inteligência Artificial possa acelerar a identificação de vulnerabilidades e apoiar a resposta a incidentes, o avanço de agentes autônomos capazes de explorar sistemas e coordenar ataques em alta velocidade amplia a desvantagem de defesa.

Os próprios sistemas de IA passaram a fazer parte da superfície de ataque. Modelos de linguagem podem ser manipulados por meio de técnicas como prompt injection, nas quais instruções maliciosas são usadas para alterar o comportamento esperado do sistema.

O tema aparece entre os principais riscos identificados pelo OWASP Top 10, documento de referência que reúne as dez categorias de riscos mais críticos à segurança de aplicações web.

“A IA pode ajudar tanto quem ataca quanto quem defende. Ao mesmo tempo em que auxilia uma organização a identificar falhas de segurança, também facilita a produção de ferramentas de ataque. É como uma faca de dois gumes”, analisa Jéferson

Nobre, professor do Instituto de Informática (INF) da Ufrgs.

Modelos de IA também podem ser manipulados e técnicas podem levar o modelo a produzir classificações incorretas e tomar decisões inadequadas. Isso acontece quando incluem situações em que o atacante modifica deliberadamente uma entrada para induzir um modelo de IA a produzir uma resposta ou classificação incorreta.

Por exemplo, pequenas alterações em uma imagem podem fazer um sistema de reconhecimento classificar incorretamente um objeto ou ataques de envenenamento de dados, nos quais dados maliciosos são introduzidos no treinamento para comprometer o comportamento futuro do modelo.

Esses ataques são preocupantes quando a IA é utilizada em aplicações críticas, como no processamento de imagens médicas ou na condução de um veículo autônomo.

Esse risco ganha dimensão com o avanço do chamado vibe



Risco ganha dimensão com chamado vibe coding, afirmam especialistas da Ufrgs

coding, prática em que o usuário descreve em linguagem natural o que deseja e utiliza a IA para gerar e modificar o código. A popularização de plataformas que geram códigos, sites e aplicativos reduz a barreira técnica, fazendo com que sistemas sejam coloca-

dos no ar sem avaliação adequada. “Já existem agentes de IA que passaram a orquestrar ataques por conta própria”, comenta Alberto Schaeffer Filho, que também é professor do INF.

A IA autônoma está assumindo o protagonismo. Em julho

de 2026, a OpenAI foi protagonista de um incidente sem precedentes. Durante testes internos, agentes de IA desenvolvidos pela empresa conseguiram contornar mecanismos destinados a isolá-los da internet e escaparam do ambiente controlado.

Apple amplia oferta para casa inteligente com HomeView

A Apple apresentou ao mercado nesta semana novos dispositivos inteligentes para a casa. A grande atração é o HomeView que chega em quatro cores, prata, estelar, rosa e cinza-espacial, e foi projetado para ser o centro da casa.

Com uma tela Liquid Retina de 7 polegadas, o dispositivo reproduz músicas, faz chamadas via FaceTime e monitora a casa por meio de automações por comando de voz.

O HomeView reconhece os usuários pelo rosto. O sistema conta com uma nova versão da Siri AI. Quando emparelhado com um dispositivo compatível com o Apple Intelligence, utiliza o contexto pessoal do usuário – como informações do Calendário, Mensagens e dados relevantes de outros apps. O HomeView pode ser colocado sobre uma mesa ou fixado na parede. A disponibilidade 13 de novembro. O valor é de US\$ 299.

APPLE/DIVULGAÇÃO/JC



Dispositivo estará disponível a partir de 13 de novembro por US\$ 299

Cazoolo avança em embalagens circulares

O Cazoolo, lab de design de embalagens circulares da Braskem, está completando quatro anos com foco na transformação da circularidade das embalagens.

O balanço dos quatro anos soma 1.100 empresas conectadas em atividades de capacitação e participação no desenvolvimento de mais de 70 soluções no mercado, em um modelo de inovação colaborativa.

Entre os resultados, o laboratório conseguiu reduzir de quatro para dois anos o ciclo total de desenvolvimento de embalagens, período que abrange desde o briefing inicial até a chegada do produto à gôndola.

Apenas na etapa de conceituação, desafios que antes podiam levar de 12 a 18 meses para serem definidos passaram a ser estruturados em cerca de duas semanas, com a entrega de protótipos em aproximadamente 45 dias.

“A principal transformação que o Cazoolo trouxe foi

acelerar, de forma clara e objetiva, a conceituação de embalagens circulares”, destaca Pier Pesce, head do Cazoolo e líder de Desenvolvimento de Negócios em Economia Circular na Braskem.

Um exemplo dessa mudança de cultura no design é o projeto em parceria com a Danone, a Graham Packaging e a Amazu. Durante um sprint de cinco dias focado na economia circular e na biomimética (criação de soluções inspiradas no funcionamento da natureza), o grupo redesenhou uma embalagem de bebida láctea inspirando-se na estrutura hexagonal das colmeias.

Ao pensar na eficiência desde o primeiro esboço, o padrão reduziu o peso da embalagem em 8%, mantendo todo o seu desempenho estrutural.

Para garantir que essas decisões sejam tomadas na origem, o programa Circular Design Sprint do lab combina a metodologia de Design for Environment e a Avaliação de Ciclo de Vida.

Loopia capta R\$ 6,5 milhões e amplia atuação

A Loopia, empresa especializada em agentes de IA para e-commerce e marketplaces, acaba de inaugurar duas novas sedes. Uma na cidade catarinense de Brusque e a outra na capital paulista.

Após a captação de R\$ 6,5 milhões em uma rodada Seed, liderada pela Parceiro Ventures, em junho, o foco agora é ampliar a equipe, estruturar as novas áreas da operação e acelerar o desenvolvimento de produtos e integrações.

A expectativa é encerrar 2026 com o dobro de colaboradores que iniciaram o ano na operação, crescimento de 300% de clientes na base e aumento de 460% na receita.

Nos últimos meses, a empresa expandiu seu ecossistema de integrações e passou a conectar sua tecnologia a plataformas como Amazon, Magalu, Mercado Livre, Shopee, Nuvemshop, Tray, Shopify, Magazord e WhatsApp.