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 mal configurada poderá paralisar a infraestrutura de um país?

Serviços vitais podem ser afetados; interpretação errônea de dados e ações inseguras são riscos

Até 2028, Inteligência Artificial (IA) mal configurada em sistemas ciberfísicos (CPS) provocará a paralisação de infraestrutura crítica nacional em pelo menos um país do G-20, projeta o Gartner, empresa de insights de negócios e tecnologia.

Os CPS são sistemas como os de automação industrial, Internet Industrial das Coisas (IIoT), robôs e drones, que orquestram sensoriamento, computação, controle, rede e análise para interagir com o mundo físico, incluindo seres humanos. "A próxima grande falha de infraestrutura pode não ser causada por hackers ou desastres naturais, mas sim por um engenheiro bem-intencionado, um script de atualização com falhas ou um decimal posicionado incorretamente", relata o vice-presidente analista do Gartner, Wam Voster.

A Inteligência Artificial mal configurada pode desligar de forma autônoma serviços vitais, interpretar erroneamente os dados dos sensores ou desencadear ações inseguras. Isso pode resultar em danos físicos ou interrupções de serviços em grande escala, representando ameaças diretas à segurança pública e à estabilidade econômica ao comprometer o controle de sistemas essenciais, como redes elétricas ou plantas industriais.

As redes elétricas modernas, por exemplo, dependem da IA para equilibrar em tempo real a geração e o consumo. Um modelo preditivo mal configurado pode interpretar erroneamente a demanda como instabilidade, acionando desnecessariamente o isolamento da rede ou o corte de carga em regiões inteiras ou até mesmo em países.

"Os modelos modernos de IA são tão complexos que muitas vezes se assemelham a caixas pretas'", diz Voster. "Mesmo os desenvolvedores nem sempre conseguem prever como pequenas alterações na configuração afetarão o comportamento emergente do modelo", acrescenta.

ADOBESTOCK/DIVULGAÇÃO/JC

Alerta vem do Gartner, empresa de insights de negócios e tecnologia

Quanto mais opacos esses sistemas se tornam, maior é o risco representado por uma configuração incorreta. Portanto, é ainda mais importante que os seres humanos possam intervir quando necessário.

O que o Gartner recomenda para os Chief Information Security Officers (CISOs) mitigarem os riscos:

- Implementar modos de sobreposição seguros: para todas as infraestruturas críticas CPS, incluir um mecanismo de desligamento de emergência seguro (kill-switch) ou outros mecanismos de sobreposição acessíveis apenas a operadores autorizados, para que os seres humanos mantenham o controle final, mesmo durante a autonomia total.

- Gêmeos digitais: desenvolver um gêmeo digital em escala real dos sistemas que suportam infraestruturas críticas para testes realistas de atualizações e alterações nas configurações antes da implementação.

- Monitoramento em tempo real: exigir monitoramento em tempo real com mecanismos de reversão para alterações feitas na Inteligência Artificial em CPS, garantindo também a criação de equipes nacionais de resposta a incidentes de IA.

> A próxima grande falha de infraestrutura pode não ser causada por hackers ou desastres naturais, mas sim por um engenheiro bem-intencionado, um script de atualização com falhas ou um decimal posicionado incorretamente"

Trojan brasileiro é a maior ciberameaça financeira

Uma evolução do GoPix, trojan bancário brasileiro, se consolida como a ciberameaça financeira mais avançada do País. O malware utiliza uma técnica única de redirecionamento de sites, explorando uma ferramenta legítima, o que dificulta a detecção pelos sistemas de segurança. Nesta nova versão, passou a incluir também alterações em boletos e criptomoedas, ampliando ainda mais seu alcance e impacto, alerta a Kaspersky.

"O GoPix representa um salto na engenhosidade dos trojans bancários brasileiros. Ele consegue operar diretamente da memória do computador, deixando pouquíssimos rastros, o que dificulta a detecção", comenta Fabio Assolini, diretor da Equipe Global de Pesquisa e Análise da Kaspersky para a América Latina e Europa.

O trojan se espalha por anúncios pagos maliciosos no Google Ads, disfarçados de serviços populares como WhatsApp, Google Chrome ou Correios, que direcionam para sites criados pelos cibercriminosos. A ameaça ataca, especificamente, alvos brasileiros em computadores e notebooks Windows, operando furtivamente da memória para roubar dados e manipular transações Pix de empresas, além de boletos e criptomoedas de usuários, sem que a vítima perceba.

A infecção inicia quando o usuário, ao pesquisar algo no Google, clica em um anúncio pago que o direciona para um site criado pelos cibercriminosos. Este site faz uma triagem inicial para verificar se o usuário é um alvo de interesse: um cliente de instituições financeiras brasileiras; um usuário de criptomoedas; ou pertence a órgãos financeiros de governos estaduais e grandes corporações.

Simpress inaugura hub e reforça posição no RS

Player de outsourcing (venda, locação e gestão) de equipamentos de TI, a Simpress encerrou 2025 no Estado com crescimento de 18% em relação ao mesmo período do ano anterior. O desempenho estadual superou a média nacional da companhia, cujo avanço foi de 11%. O destaque foi o pilar de Automação, composto por coletores de dados e impressoras térmicas, com expansão de 62%. "O desempenho alcançado no Rio Grande do Sul reforça o potencial da região e a capacidade da Simpress em oferecer soluções completas e inovadoras em outsourcing de TI", destaca o diretor comercial da Simpress, Fernando Danesi.

SIMPRESS/DIVULGAÇÃO/JC

Fernando Danesi é diretor comercial da Simpress

Quer receber notícias de inovação e tecnologia? Cadastre-se no Bot do **Mercado Digital**!