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

MICROSOFT/DIVULGAÇÃO/JC

Temos que nos proteger da IA e usar IA para nos proteger, diz Toledo

André Toledo, líder de Segurança da Microsoft Brasil, destaca as vulnerabilidades em ambientes corporativos

A Inteligência Artificial já não é apenas uma ferramenta de apoio ao trabalho. Com a expansão dos agentes de IA, capazes de executar tarefas, acessar informações e automatizar rotinas, ela passa a operar dentro dos ambientes corporativos com um nível de autonomia que exige atenção redobrada das empresas.

Para André Toledo, líder de Segurança da Microsoft Brasil, o avanço abre uma nova frente de risco: é preciso proteger a IA, mas também usar a própria IA para ampliar a capacidade de defesa.

A aceleração dos ataques cibernéticos nos últimos anos mostra que os criminosos digitais acompanham rapidamente cada mudança tecnológica. A partir da pandemia, quando os profissionais passaram a trabalhar em ambientes fora das empresas, as ferramentas de segurança precisaram se adaptar a essa nova realidade, que potencializa os riscos, principalmente de ataques relacionados à identidade dos usuários dos sistemas.

Toledo costuma traduzir essa escalada fazendo alusão ao bater de asas de um beija-flor, que, dependendo da espécie, pode fazer o movimento 80 vezes por segundo. Em 2020, os ataques de identidade já ocorriam em velocidade sete vezes maior: eram 575 ataques por segundo. No ano passado, esse número chegou a 4 mil. Agora, são 7 mil ataques de identidade por segundo.

Se antes muitos ataques buscavam explorar brechas dos sistemas, hoje os criminosos perceberam que invadir uma organização "legitimamente", usando credenciais, senhas e identidades comprometidas, pode ser mais barato e eficiente. Com a IA, esse cenário se tornou mais complexo. A tecnologia aumenta capacidades humanas – e isso vale também para quem ataca.

"A primeira dificuldade é que já fica difícil de identificar um e-mail legítimo e não legítimo. Outra coisa que começou a ser feita é a automatização de ataques: um código malicioso que precisava ser comprado de um outro desenvolvedor, agora ele [cibercriminoso] consegue produzir o próprio", detalha, Toledo. Segundo ele, os criminosos também já usam IA para analisar códigos legados e identificar vulnerabilidades em ambientes que não foram devidamente isolados ou protegidos.

> Um código malicioso que precisava ser comprado de um outro desenvolvedor, agora ele [cibercriminoso], consegue produzir o próprio

Outro ponto de atenção é o chamado shadow AI. Assim como profissionais passaram a contratar serviços em nuvem sem a governança da área de tecnologia, agora muitos usam ferramentas gratuitas de IA para acelerar o trabalho sem avaliar os riscos envolvidos. O problema é que, em alguns serviços, as informações inseridas podem ser usadas para treinar modelos, principalmente quando os serviços são gratuitos.

"Se você não está pagando o serviço, é porque você é o produto", alerta Toledo. Nesse contexto, cresce o risco de vazamento de informações, um problema que compromete, inclusive, o cumprimento das regras previstas na Lei Geral de Proteção de Dados (LGPD).

'As pessoas é que são as responsáveis pelos seus agentes'

O desafio é ainda maior porque a IA introduz novas formas de ataque. Modelos de linguagem não diferenciam, por natureza, dado e instrução da mesma forma que um sistema tradicional. Tudo pode ser interpretado como texto a ser processado. Isso abre espaço para ataques em que instruções maliciosas são inseridas em sites, documentos ou até conteúdos aparentemente invisíveis, para que a IA as leia e execute sem que o usuário perceba. Por isso, Toledo defende que antes de escalar projetos de IA, as empresas precisam revisar permissões, classificar dados, definir políticas de uso e aplicar controles de segurança desde o início.

A lógica do Zero Trust, que ganhou força com o trabalho remoto, também deve orientar a criação e o uso de agentes de IA. A ideia é conceder apenas acessos necessários, monitorar atividades e estabelecer barreiras para reduzir danos em caso de falha ou ataque, porque a responsabilidade é de quem opera a ferramenta.

"De maneira alguma, numa apresentação eu posso falar que um dado está errado porque o agente errou. As pessoas são responsáveis pelo seu agente", exemplifica Toledo. Essa lógica também vale para as lideranças, que precisam se comprometer com a questão da segurança. Para enfrentar esse novo estágio da segurança digital, a Microsoft lança em maio o Agent 365, solução criada para ampliar a governança sobre agentes de IA. O objetivo é permitir que as organizações acompanhem o comportamento dessas automações, compreendam seus acessos e estabeleçam limites. "Estamos entrando em uma nova onda de adoção da IA. E, nesses ciclos, a segurança precisa estar embarcada desde o início."

PENSE RÁPIDO

com Eduardo Vieira, sócio do SoftBank na América Latina

SARAH OLIVEIRA/DIVULGAÇÃO/JC

Qual é o maior risco invisível que as startups ignoram hoje em dia?
Não investir na sua marca e na sua reputação, achando que isso vai ser uma coisa para pensar só lá na frente. Tem que investir desde o dia zero.

Em um mundo onde a tecnologia é abundante, qual tem que ser o foco do empreendedor para ele não desenvolver algo que fique datado rapidamente?
Focar no que não muda. Ao invés de ficar preocupado com FOMO (Fear of Missing Out), foca nas coisas que você tem certeza que não vão mudar, porque o resto é só ruído, só barulho.

Em que momento o investidor tem que parar de apoiar e passar a pressionar o empreendedor?
A relação investidor e founder é um casamento. Você apoia e pressiona o tempo inteiro. É uma convivência com altos e baixos, então, não tem só o momento de apoiar ou de pressionar, tem que ser a harmonia.