Opinião

A vulnerabilidade não está mais no código, mas em quem tem acesso a ele

Bruno Kaique (*)

Um desenvolvedor recebe um alerta de falha no pipeline e faz o que faria em qualquer outro dia: revisa o processo, autentica o acesso e segue o fluxo. Minutos depois, sem perceber, abriu acesso para um invasor no ambiente de desenvolvimento.

Esse tipo de situação deixou de ser pontual — e revela uma mudança mais profunda. O uso indevido de credenciais tem acompanhado a evolução dos ataques cibernéticos e já aparece com frequência em incidentes relevantes. O relatório *Cost of a Data Breach*, da IBM, destaca a importância de fortalecer controles de identidade e acesso para reduzir o risco de abuso de credenciais.

Esse cenário ganhou evidência recente no Brasil. Em 2025, um ataque a uma empresa parceira do Banco Central resultou em desvios milionários após o uso indevido de credenciais legítimas. O caso não envolveu falhas na infraestrutura do Banco Central, mas sim o comprometimento de acessos.

O atacante não precisa mais explorar vulnerabilidades. É mais simples explorar identidades válidas e credenciais legítimas, operando sem levantar suspeitas e, muitas vezes, realizando movimentação lateral entre sistemas. E os pipelines de desenvolvimento tem se mostrado um campo muito fértil para essas explorações.

O novo perímetro deixou de ser técnico

Durante muito tempo, a segurança foi tratada como um problema de código e infraestrutura. Falhas eram corrigidas, sistemas atualizados e o foco estava na superfície técnica.

Esse modelo ainda é necessário, mas já não é suficiente. O perímetro mudou e hoje está diretamente ligado à gestão de identidades e acessos (IAM) e a quem interage com ambientes críticos.

Desenvolvedores concentram acessos sensíveis ao longo da operação, incluindo repositórios de código, pipelines de CI/CD, ambientes de teste e produção, chaves de API e configurações em nuvem. Quando uma dessas identidades é comprometida, o impacto deixa de ser pontual. O invasor passa a operar com credenciais válidas e se movimenta lateralmente, ampliando alcance sem necessariamente gerar alertas.

Ataques não exploram falhas, exploram contexto

Grande parte desses acessos não vem de técnicas sofisticadas, mas de abordagens que exploram o contexto de trabalho. O phishing direcionado a desenvolvedores segue essa lógica.

São mensagens que reproduzem a rotina, como convites para repositórios, notificações de versionamento ou alertas de falha em pipelines. Tudo parece legítimo porque replica fluxos reais de desenvolvimento.

Quando a interação acontece, o atacante não precisa contornar controles. Ele passa a operar com credenciais válidas dentro do fluxo esperado.

Isso reduz a capacidade de detecção, já que muitos controles ainda estão focados em identificar comportamentos anômalos e não o uso indevido de identidades legítimas.

A cadeia de software amplia o impacto

O risco cresce com a cadeia de suprimentos de software. Aplicações modernas dependem de bibliotecas open source, componentes de terceiros e integrações contínuas, ampliando a superfície de ataque.

Uma única dependência comprometida pode afetar diversas organizações ao mesmo tempo. Um pacote malicioso ou atualização adulterada pode inserir código nocivo diretamente na distribuição de aplicações, propagando o risco em escala.

O risco hoje está na interseção entre tecnologia, identidade e comportamento. Controles tradicionais continuam sendo fundamentais, mas não são suficientes para mitigar ataques que exploram credenciais legítimas dentro do fluxo normal de trabalho.

Proteger software agora é proteger acesso

Proteger o software passa por proteger o ambiente de desenvolvimento. Isso envolve reduzir privilégios excessivos, fortalecer políticas de gestão de identidade e acesso, monitorar padrões de uso de credenciais e adotar práticas contínuas de governança.

Também exige preparar desenvolvedores para reconhecer ataques que simulam o próprio fluxo de trabalho, um tipo de ameaça que não depende de vulnerabilidades técnicas, mas de contexto operacional.

Segurança começa nas pessoas que sustentam o código

O avanço do DevSecOps elevou o nível técnico da segurança, mas também evidenciou uma mudança de perspectiva. Software não é apenas código, é resultado de decisões humanas.

Desenvolvedores e equipes de engenharia fazem parte da base de confiança que sustenta a operação digital. Ignorar esse fator é manter aberta uma das superfícies de ataque mais eficientes hoje.

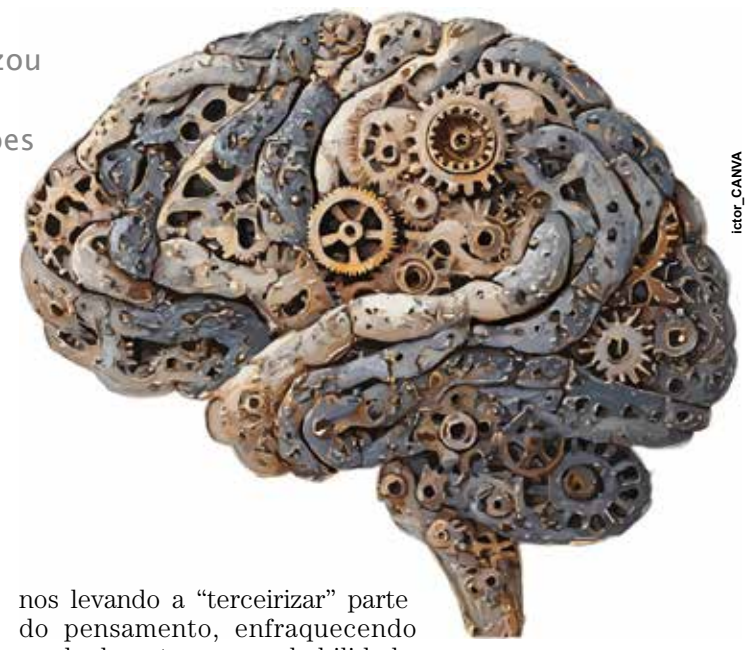
Proteger aplicações não é apenas corrigir vulnerabilidades. É proteger quem tem acesso direto a elas.

(*) CTO da Beephish.

Mais um estudo liga inteligência artificial a problemas cognitivos

No ano passado, uma equipe de pesquisadores do MIT liderada pela cientista Nataliya Kosmyna, utilizou eletroencefalogramas para monitorar a atividade cerebral de estudantes enquanto escreviam redações curtas, com temas abertos.

Vivaldo José Breternitz (*)



ictor_CANVA

Os 54 participantes foram divididos em três grupos: um deveria usar o ChatGPT, outro podia recorrer ao Google, mas sem usar os resumos gerados por inteligência artificial e o terceiro precisava confiar apenas em seus próprios conhecimentos. Cada grupo produziu uma redação por mês, durante três meses. No quarto mês, parte dos estudantes foi instruída a mudar de estratégia, passando a usar ou deixando de usar o ChatGPT.

Os resultados do experimento, descritos em um artigo ainda não revisado por pares, foram preocupantes. Segundo os pesquisadores, os alunos que recorreram ao ChatGPT "apresentaram desempenho consistentemente inferior nos níveis neural, linguístico e comportamental" e tornaram-se mais preguiçosos a cada nova redação. "O cérebro não chegou a "adormecer", mas houve muito menos ativação nas áreas ligadas à criatividade e ao processamento de informações", disse Kosmyna em entrevista à BBC.

Além disso, os participantes que usaram o chatbot tiveram dificuldade em citar trechos de seus próprios textos, o que reforça estudos anteriores que apontam para um impacto negativo da IA na capacidade de memorização e de recuperação de informações. A questão da originalidade também surgiu: uma professora envolvida na pesquisa chegou a perguntar se os alunos que usavam o ChatGPT "estavam sentados lado a lado, porque os textos eram muito semelhantes".

O estudo funciona como um alerta para um fenômeno que começa a ser investigado: o uso intensivo de chatbots pode estar nos levando a "terceirizar" parte do pensamento, enfraquecendo gradualmente nossas habilidades cognitivas.

Pesquisadores da Universidade da Pensilvânia também observaram que, em pesquisa que desenvolveram, diante de perguntas envolvendo raciocínio e conhecimento, os participantes preferiram recorrer ao ChatGPT, comportamento que chamaram de "rendição cognitiva".

Em resumo: ainda há muito a ser compreendido sobre os efeitos da inteligência artificial na mente humana, mas, como destacou Kosmyna, é preciso investigá-los com urgência, sobretudo porque "nosso cérebro adora encontrar atalhos cognitivos".

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnitz@gmail.com.

Dell Technologies e Instituto ELDORADO inauguram primeiro laboratório global de design digital

A Dell Technologies, em parceria com o Instituto ELDORADO, anunciou nesta terça-feira (28) a criação de um laboratório de design digital no Brasil dedicado à pesquisa aplicada em inteligência artificial, experiência do usuário e inovação em design digital. Inédito em toda a operação global da companhia, o espaço será instalado no novo prédio do Instituto Caldeira, em Porto Alegre, que reúne empresas, startups e centros de pesquisa em projetos de inovação, e nasce com o objetivo de integrar capacidades industriais e científicas em um ambiente colaborativo de desenvolvimento tecnológico.

Divulgação

A concretização do projeto é fruto da colaboração entre os três parceiros que viabilizaram a iniciativa na capital gaúcha. A Dell foi a responsável pelo investimento e pela orientação estratégica das pesquisas. O Instituto ELDORADO, por sua vez, conduzirá a execução técnica dos projetos. O laboratório será instalado no novo complexo de inovação que o Caldeira está desenvolvendo nos antigos prédios da fábrica Tecidos Guahyba, em Porto Alegre, região do Quarto Distrito, que vem se consolidando como polo de inovação e economia criativa na capital gaúcha.

"O Brasil tem um papel cada vez mais relevante no desenvolvimento tecnológico global da companhia. Com este laboratório, reforçamos nosso compromisso de investir em pesquisa e inovação no país, contribuindo também para o fortalecimento do ecossistema local de tecnologia", afirma o presidente da Dell Technologies no Brasil, Diego Puerta.

Segundo Puerta, a criação do laboratório representa mais um investimento estruturante em P&D, alinhado ao compromisso de longo prazo da Dell com o país. Presente no Brasil desde 1999, a empresa vem ampliando de forma consistente sua atuação em inovação e já conta com três centros de pesquisa e desenvolvimento em solo brasileiro.

O laboratório será dedicado à investigação de novas abordagens em design digital, experiência de usuário e design de produtos para o ecossistema digital. A proposta é criar um ambiente colaborativo em que pesquisadores do Instituto ELDORADO e profissionais de design da Dell possam desenvolver estudos e experimentações que orientem decisões futuras de design da companhia e, ao mesmo tempo, ampliem o conhecimento sobre práticas, processos e tendências em design, com potencial de impacto para além do contexto corporativo.

"Essa iniciativa reforça o papel do Instituto ELDORADO como parceiro estratégico em projetos de pesquisa aplicada de alto impacto, conectando ciência, indústria e inovação em escala global", afirma Roberto Soboll, superintendente do Instituto ELDORADO.

News @ TI

ricardosouza@netjen.com.br

Lançamento de ultrassom integrado à IA

@A VX Medical Innovation, com o objetivo de apoiar a expansão do mercado brasileiro de radiologia e aprimorar seu ecossistema de soluções, apresenta durante a 56ª edição da Jornada Paulista de Radiologia (JPR), a Wind Ultrassom, nova solução que usa IA, voltada para diagnósticos por imagem. O lançamento é o principal destaque da participação da empresa mineira no evento, considerado o maior do setor de diagnóstico por imagem da América Latina. A JPR, que acontece entre os dias 30 de abril e 3 de maio, projeta reunir cerca de 100 empresas expositoras e 800 palestrantes no Transamerica Expo Center, em São Paulo. A nova solução da VX Medical Innovation chega em um momento de pressão crescente sobre a cadeia de diagnóstico por imagem no país. De acordo com dados do Atlas da Radiologia no Brasil 2025, publicado pelo Colégio Brasileiro de Radiologia (CBR), o volume de exames diagnósticos por imagem cresceu cerca de 15,6% entre 2014 e 2023, quando o país realizou aproximadamente 169,6 milhões exames, reforçando a necessidade de soluções que fortaleçam esse ecossistema (https://vx.med.br/).

Plataforma agregadora gratuita reúne imóveis em leilão de todo Brasil

@O Leilão de Imóveis é um agregador digital gratuito que reúne mais de 30 mil imóveis e organiza todas as informações em um único ambiente, permitindo pesquisar, filtrar e comparar as opções de forma mais rápida e estruturada. Desenvolvido pela Zuk, empresa referência em leilões de imóveis no Brasil e pela Arremates, plataforma de ensino voltada ao segmento leiloeiro, a nova ferramenta amplia a visibilidade sobre preços, descontos e condições dos ativos. A proposta é transformar uma busca antes dispersa em uma experiência mais eficiente. Por meio de um sistema de filtros, o usuário pode refinar a procura com base em critérios como localização, tipo de imóvel, faixa de preço, metragem, leiloeiro e data do leilão. Também é possível ordenar os resultados por valor ou nível de desconto, o que facilita a identificação de opções mais alinhadas ao perfil de cada comprador (https://www.portalzuk.com.br/) (https://arremates.com.br/).

Empresas & Negócios **José Hamilton Mancuso (1936/2017)** **Laurinda Machado Lobato (1941-2021)** Responsável: **Lilian Mancuso**

Editorias
Economia/Política: J. L. Lobato (lobato@netjen.com.br); *Ciência/Tecnologia:* Ricardo Souza (ricardosouza@netjen.com.br); *Livros:* Ralph Peter (ralphpeter@agenteliterarioralph.com.br);
Comercial: comercial@netjen.com.br
Publicidade Legal: lilian@netjen.com.br

Webmaster/TI: Fabio Nader; *Editoração Eletrônica:* Ricardo Souza.
Revisão: Maria Cecília Camargo; *Serviço informativo:* Agências Brasil, Senado, Câmara, EBC, ANSA.

Artigos e colunas são de inteira responsabilidade de seus autores, que não recebem remuneração direta do jornal.

Colaboradores: Claudia Lazzarotto, Eduardo Moisés, Geraldo Nunes e Heródoto Barbeiro.

ISSN 2595-8410

Jornal Empresas & Negócios Ltda
Administração, Publicidade e Redação: Rua Joel Jorge de Melo, 468, cj. 71 – Vila Mariana – São Paulo – SP – CEP.: 04128-080
Telefone: (11) 3106-4171 – E-mail: (netjen@netjen.com.br)
Site: (www.netjen.com.br). CNPJ: 05.687.343/0001-90
JUCESP, Nire 35218211731 (6/6/2003)
Matriculado no 3º Registro Civil de Pessoa Jurídica sob nº 103.