OPINIÃO

Os riscos da IA que roda dentro da sua empresa

Cláudio Bannwart (*)

Durante anos, empresas ao redor do mundo adotaram soluções de Software como Serviço (SaaS) e aplicações em nuvem, atraídas pela promessa de agilidade, escalabilidade e gestão simplificada.

No entanto, diante de preocupações legítimas com a segurança dos dados, muitas passaram a seguir na direção oposta para atender suas demandas de IA impulsionando as implementações locais (on-premises) dessas tecnologias.

Executar modelos de IA em infraestrutura local oferece às organizações maior controle sobre dados sensíveis, respondendo a preocupações com privacidade e soberania da informação. À primeira vista, essa abordagem parece resolver os problemas de segurança levantados por ferramentas de IA baseadas na nuvem. No entanto, ao analisarmos mais de perto essa tendência, fica claro que on-premises não significa automaticamente mais seguro. Assim como em qualquer implementação no local, a responsabilidade pela segurança recai inteiramente sobre a organização e seus usuários e, sem o envolvimento adequado das equipes de segurança, esses ambientes podem se tornar vetores significativos de risco.

Uma pesquisa recente do Netskope Threat Labs esclarece esses riscos. De acordo com o relatório, 34% das organizações no mundo já utilizam interfaces LLM on-premises, com destaque para o Ollama com 33%, seguido por LM Studio (0,9%) e Ramalama (0,6%). Além disso, 5,5% das organizações têm usuários executando agentes de IA criados com frameworks populares de agentes de IA em ambientes locais. Essas ferramentas são facilmente acessíveis aos usuários, permitindo a criação de aplicações e agentes personalizados, mas, ao contrário das plataformas SaaS gerenciadas, muitas vezes vêm com pouca ou nenhuma segurança embutida. Por exemplo, o Ollama não possui autenticação nem proteções padrão, exigindo a adição de camadas de segurança antes que seu uso seja considerado seguro.

Além disso, os modelos e ferramentas necessários para o desenvolvimento local de IA são frequentemente encontrados em marketplaces públicos, que disponibilizam recursos open source capazes de introduzir riscos significativos à cadeia de suprimentos. Atores maliciosos podem embutir códigos nocivos em modelos ou conjuntos de dados, ou explorar formatos vulneráveis como Python Pickles para executar comandos arbitrários e infiltrar a rede da organização. Já o Hugging Face, uma das plataformas mais populares para compartilhamento de modelos, dados e ferramentas de IA, é acessado por usuários em 67% das organizações, tornando-se um vetor crítico de atenção para as equipes de cibersegurança. Em outras palavras, qualquer colaborador com conhecimentos técnicos que baixe e execute um modelo não verificado pode estar abrindo as portas para um invasor.

Os próprios modelos ou agentes de IA também representam riscos à segurança da informação. A maioria requer acesso direto e interação com fontes de dados corporativos para treinamento ou execução de tarefas, e seus níveis de permissão devem ser restritos para evitar a exposição de dados sensíveis durante suas operações.

O problema é que essas implementações locais de IA muitas vezes ocorrem sem a visibilidade e o controle das equipes de TI e segurança cibernética. Não se pode proteger aquilo que não se conhece, e essas plataformas, modelos ou agentes locais podem ser utilizados sem as devidas barreiras de proteção.

À medida que mais pessoas conduzem esses experimentos, o fenômeno da "Shadow AI" e os riscos à segurança dos dados tendem a se intensificar, a menos que as equipes de segurança atuem de forma proativa para identificar e controlar esses usos.

A solução não está em proibir completamente o uso de IA on-premises. Na maioria dos casos, os colaboradores essas ferramentas com foco em produtividade, algo que, inclusive, está alinhado à estratégia de muitas organizações. O papel das equipes de segurança, portanto, deve ser adotar uma abordagem mais equilibrada de "capacitação segura", garantindo que a segurança atue como facilitadora da inovação, e não como barreira. A prioridade deve ser eliminar a Shadow AI, identificando quem está usando essas ferramentas e de que forma. Isso exige capacidades de segurança que ofereçam visibilidade total e controle sobre tráfego, rede, usuários e dados, em ambientes de nuvem e on-premises. Com a visibilidade estabelecida, é possível implementar os controles adequados para assegurar o desenvolvimento e uso da IA de forma segura e responsável.

Existem diversas estruturas de segurança, como o projeto OWASP GenAI Security e a matriz ATLAS, que oferecem orientações valiosas para antecipar os riscos associados à inovação em IA. Essas estruturas abordam pontos críticos como injeção de comandos, vazamento de dados e ameaças à cadeia de suprimentos.

Por fim, é essencial reforçar a compreensão de que, embora a proposta da IA local seja promissora, a busca por inovação não pode comprometer a segurança. Ao identificar e proteger proativamente essas implementações, as organizações podem continuar inovando enquanto preservam seu bem mais valioso: os dados.

(*) Country manager da Netskope no Brasil.

China lança data center submarino alimentado por energia eólica

A China anunciou o lançamento do primeiro data center subaquático do mundo, instalado a 35 metros de profundidade na costa de Xangai, resfriado pela água do mar e alimentado por energia eólica.

Vivaldo José Breternitz (*)

O projeto, no qual foram investidos US$ 226 milhões, tem como objetivo economizar energia elétrica, um insumo cada vez mais importante em data centers, onde é utilizada para refrigeração e atividades de processamento de dados propriamente ditas.

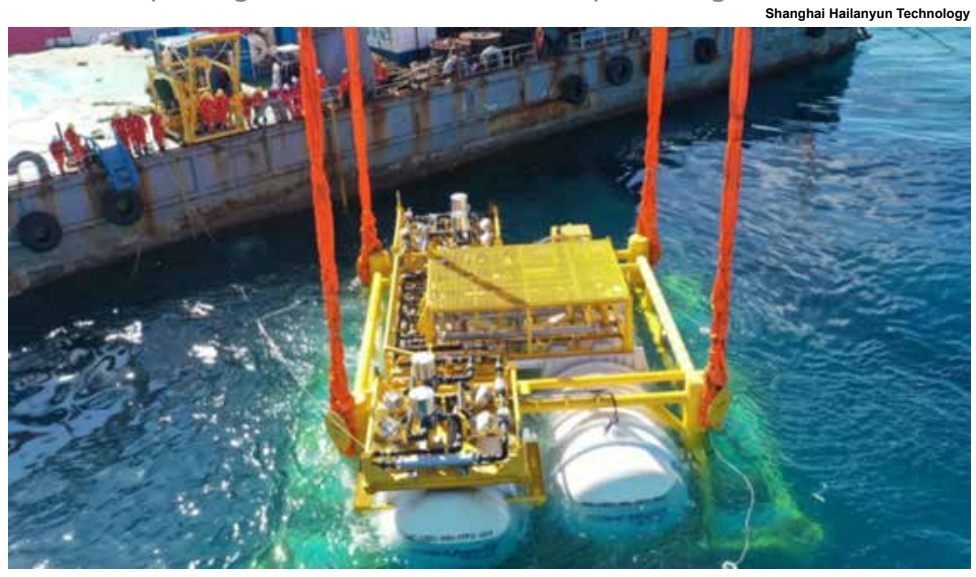
A energia elétrica tornou-se um fator tão importante na área a ponto da capacidade dos data centers agora ser expressa em megawatts (MW), unidade de potência elétrica. Na atualidade, já há data centers que exigem 100 MW, o equivalente ao consumo de uma cidade de 50 mil habitantes.

Segundo os responsáveis pelo projeto, a primeira fase deste já está operacional com capacidade de 2,3 MW, devendo chegar a 24 MW, sendo que já está em estudo uma versão de 500 MW a ser instalada em alto-mar.

Vale lembrar que entre 2018 e 2020, para fins de pesquisa, a Microsoft manteve o Natick, um data center submarino instalado nas costas da Escócia; no entanto, o projeto foi encerrado em função de seus custos e dificuldades de manutenção.

Conceitualmente, o projeto é simples: instalar os servidores em cápsulas hermeticamente fechadas, submergi-los no leito marinho e deixar que o oceano absorva o calor gerado - isso deve levar a um índice de eficiência energético (Power Usage Effectiveness - PUE) inferior a 1,15, melhor que a média dos grandes data centers terrestres e abaixo do mínimo exigido na China, 1,25.

Shanghai Hailanyun Technology



As capsulas são revestidas com material anticorrosivo para resistir ao ambiente salino, sendo a manutenção e atualização de hardware um processo caro e demorado. Escalar o projeto para centenas de MW em profundidades maiores pode ampliar significativamente esses fatores.

Ecologistas manifestaram suas preocupações com possíveis impactos de data centers como esse sobre o meio ambiente, especialmente se seu uso se disseminar e propõem pesquisas a respeito antes de que isso aconteça.

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

Com 36 mil alunos já certificados, Hackers do Bem abre mais 25 mil vagas

"Acreditava que, aos 60 anos, era tarde para aprender algo completamente novo. Mas esta oportunidade me mostrou que nunca é tarde para recomeçar". A afirmação é de Marcelo Goulart, um dos 216 participantes da Residência Tecnológica, última etapa do programa Hackers do Bem. A iniciativa do Ministério da Ciência, Tecnologia e Inovação (MCTI) executada pela RNP (Rede Nacional de Ensino e Pesquisa) visa formar profissionais qualificados para o concorrido mercado de cibersegurança. O curso gratuito está com inscrições abertas para 25 mil novas vagas nos cursos de nivelamento e básico.

O programa oferece ampla capacitação, começando por temas introdutórios à área de cibersegurança até conteúdos mais avançados, como a identificação de ameaças cibernéticas, computação em nuvem, conceitos de desenvolvimento e aplicações de criptografia. Conheça mais detalhes sobre as formações. Desde seu lançamento, em janeiro de 2024, o Hackers do Bem já certificou mais de 36 mil alunos.

A última etapa do Hackers do Bem é a Residência Tecnológica, momento bastante esperado pelos participantes para atuar de forma prática na solução de problemas cibernéticos dentro dos Pontos de Presença da RNP, nos mais diversos estados do Brasil. Nesta fase, os alunos recebem bolsa-auxílio mensal de R$ 3 mil por um semestre. É a oportunidade para muitos se especializarem na área e até realizarem o sonho da transição de carreira para uma profissão com altas e crescentes expectativas de demanda.

anyaberkut_CANVA

De acordo com o relatório global sobre a lacuna de habilidades em segurança cibernética de 2024, divulgado pela Fortinet, seriam necessários atualmente quatro milhões de profissionais de cibersegurança no mundo para mitigar os riscos e lidar com as diferentes ameaças digitais.

Goulart, morador de Alto Paraíso de Goiás (GO), começou sua carreira na área de tecnologia como programador. Ele conta que encontrou no Hackers do Bem uma nova direção profissional.

"Descobri o programa ao ouvir a ministra Luciana Santos falando sobre ele. Desde então, me dediquei aos estudos e me surpreendi com o nível do material e das aulas online. Agora, com um grupo de colegas, estou elaborando um projeto cooperativo em segurança cibernética", explica. Para ele, é uma oportunidade de consolidar a transição de carreira. "Quero ser um pentester ou até mesmo gerenciar projetos na área", conta.

Aos 52 anos, Patrícia Monfardini é um exemplo de resiliência entre os candidatos que foram até a última etapa. Sem experiência prévia em tecnologia, ela se inscreveu no programa por incentivo de uma colega de trabalho.

"Foi um desafio enorme. Não sabia nada sobre TI, mas, com muita persistência, cheguei à especialização no Red Team (segurança ofensiva). Chorei, estudei e, no final, venci," comemora. Patrícia vê na Residência Tecnológica a chance de colocar em prática o que aprendeu e fazer a transição da carreira atual, como servidora pública em Contagem (MG), para a área de cibersegurança. A aluna mineira, inclusive, após se formar no Hackers do Bem, começou a cursar Engenharia de Software para seguir na área depois da experiência no programa.

Além de formar profissionais tecnicamente preparados para lidar com os mais diversos golpes digitais, o Hackers do Bem busca aumentar a conscientização sobre a importância da segurança digital em um mundo cada vez mais conectado. "Muitas pessoas ignoram o quanto é necessário proteger nossas informações, mas o programa pode mudar isso. É uma iniciativa que não só prepara indivíduos, mas fortalece toda a sociedade", diz Patrícia (https://hackersdobem.org.br/).

News @TI

ricardosouza@netjen.com.br

Anatel homologa roteador Wi-Fi 7 da Blu-Castle para ultrabanda residencial

@A Blu-Castle acaba de homologar na Anatel o seu novo roteador GPON com tecnologia Wi-Fi 7. O produto vem para atender o mercado residencial e de pequenas empresas com demanda de serviços digitais premium. Ele suporta a conexão simultânea de até 250 dispositivos de usuários de consumo massivo e recebeu uma configuração especialmente dimensionada para as necessidades econômicas e de infraestrutura do mercado nacional. Segundo a Blu-Castle, este é o primeiro Wi-Fi 7 homologado para o Brasil na categoria de equipamentos Dual Band 4X4, apresentando um custo inicial até 20% menor para provedores e operadoras locais na comparação com as demais alternativas disponíveis (www.blu-castle.com).

Líderes femininas de TI se reúnem em SP

@Em meio a um cenário em que profissionais buscam cada vez mais propósito e sentido no trabalho, líderes femininas da tecnologia vão se reunir em São Paulo para discutir como criar ambientes motivadores e alinhados a valores compartilhados. O TechConnect Women's Edition, marcado para 4 de novembro, reunirá representantes de comunidades como Ser Mulher em Tech, Mulheres na IA, Mulheres de Produto, TI de Salto, MCIO e Rede Mulher Empreendedora (RME), além de executivas de empresas como IBM, Nubank e Microsoft. A iniciativa acontece em um contexto global em que o propósito e o alinhamento de valores impactam diretamente a satisfação e o desempenho profissional (https://techconnect.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.