



OPINIÃO

Estratégias prioritárias para CIOs em um cenário de ameaças avançadas

Paulo Lima (*)

À medida que o ano de 2025 avança, a segurança da informação continua a ser uma prioridade estratégica para as organizações.

Com o aumento das ameaças cibernéticas, a transformação digital acelerada e a pressão regulatória crescente, os CIOs enfrentam o desafio de proteger dados e ativos críticos enquanto impulsionam a inovação. Este artigo explora as principais tendências em segurança da informação que estão moldando o cenário corporativo e como os líderes de tecnologia podem se preparar para os desafios e oportunidades que elas apresentam.

O modelo de segurança Zero Trust, que se baseia no princípio de "nunca confiar, sempre verificar", continua ganhando força. Segundo um relatório da Forrester, 76% das organizações globais estão em processo de implementação ou planejam fazê-lo nos próximos 12 meses. Essa abordagem é essencial para proteger ambientes corporativos modernos, onde as fronteiras tradicionais de rede estão desaparecendo devido ao trabalho remoto e ao uso de dispositivos móveis.

Para os CIOs, a implementação de Zero Trust envolve a adoção de tecnologias como autenticação multifatorial, controle de acesso baseado em políticas e monitoramento contínuo de atividades. Além disso, é fundamental promover uma cultura organizacional que compreenda e apoie os princípios do modelo de cibersegurança.

A integração de Inteligência Artificial (IA) e Machine Learning (ML) em soluções de segurança também estão transformando a maneira como as organizações detectam e respondem a ameaças. Ferramentas baseadas em IA e ML podem analisar grandes volumes de dados em tempo real, identificar padrões anômalos e automatizar respostas a incidentes. De acordo com a Gartner, até 2025, as empresas que investirem nelas estarão à frente de 95% das atividades de monitoramento e resposta a ameaças em empresas maduras em cibersegurança.

Investir em soluções que incorporam IA e ML pode melhorar significativamente a eficiência operacional, reduzir o tempo de resposta a incidentes e fortalecer a postura de segurança da organização.

Com a crescente adoção de ambientes multinuvem, garantir a segurança em diferentes plataformas de nuvem tornou-se um desafio significativo.

Segundo a IDC, mais de 80% das grandes empresas globais estarão utilizando ambientes multinuvem até o final de 2025. Isso exige soluções de segurança que ofereçam visibilidade e controle centralizados sobre as infraestruturas na nuvem, além de garantir conformidade e mitigar riscos.

Além disso, é preciso considerar a implementação de ferramentas como Cloud Access Security Brokers (CASBs), firewalls de próxima geração e soluções de monitoramento contínuo para proteger dados e aplicações em ambientes multinuvem.

Os ataques de ransomware continuam a ser uma das maiores ameaças para as organizações. Em resposta, a estratégia de cibersegurança deve incluir medidas robustas de backup e recuperação. Utilizar soluções de Backup as a Service (BaaS) pode ajudar a garantir a proteção de dados críticos e a rápida restauração em caso de ataque.

Além disso, a construção de uma cultura de resiliência cibernética é essencial. Isso envolve a preparação para incidentes, a implementação de planos de resposta a incidentes e a realização de exercícios de simulação para testar a eficácia das estratégias de recuperação.

Com regulamentações como a LGPD (Lei Geral de Proteção de Dados) no Brasil e o GDPR na Europa, as organizações devem garantir que suas práticas de segurança de dados estejam em conformidade com as leis de privacidade. Implementar soluções de Identity Access Management (IAM) e realizar auditorias regulares são passos cruciais para evitar penalidades e proteger os dados dos clientes.

Por isso é importante reforçar que os CIOs devem trabalhar em estreita colaboração com as equipes jurídicas e de conformidade para garantir que as políticas e práticas de segurança atendam aos requisitos regulatórios aplicáveis.

Em 2025, os CIOs desempenham um papel fundamental na proteção das organizações contra ameaças cibernéticas e na promoção de uma cultura de segurança. Ao adotar abordagens estratégicas, investir em tecnologias emergentes e colaborar com outras áreas da organização, os líderes de tecnologia podem fortalecer a postura de segurança e garantir a continuidade dos negócios em um ambiente digital cada vez mais complexo.

(*) CEO da Skymail, empresa destaque em serviços de e-mail corporativo, cloud computing e segurança digital.

IA e desemprego: Huang critica Amodei

O evento VivaTech, recentemente acontecido em Paris, é um dos maiores eventos de inovação e tecnologia da Europa

Vivaldo José Breternitz (*)

Durante sua participação no evento, o CEO da Nvidia, Jensen Huang, criticou duramente o diretor-executivo da Anthropic, Dario Amodei, por declarações recentes nas quais este previu que a inteligência artificial poderá eliminar 50% dos empregos administrativos de nível inicial, levando a uma taxa de desemprego de até 20% nos próximos cinco anos.

Segundo a revista *Fortune*, o CEO da Nvidia afirmou que “discorda praticamente de tudo” o que Amodei disse. Disse Huang: “Primeiro: ele acredita que a IA é tão assustadora que só eles [a Anthropic] deveriam desenvolvê-la. Segundo, que a IA é tão cara que mais ninguém deveria tentar. Terceiro, que a IA é tão poderosa que todo mundo perderá o emprego — o que justificaria que apenas eles construam esse tipo de tecnologia” — com ironia, foram as palavras de Huang.

Continuando, disse o CEO da Nvidia: “Acredito que a IA é uma tecnologia muito importante, e devemos desenvolvê-la de forma segura e responsável. E, para que isso aconteça, tem que ser feito às claras... não se faz isso numa sala escura dizendo que está tudo seguro.”

A Anthropic foi fundada por Amodei em 2021, ao lado de ex-funcionários da OpenAI, após divergências sobre a direção e as práticas de segurança da empresa. Desde então, a Anthropic tem se posicionado



demaerre_CANVA

como uma companhia voltada ao desenvolvimento ético e seguro da IA. Seu modelo mais recente, o Claude 4 Opus, demonstrou capacidades avançadas, incluindo escrever código em nível quase humano e realizar ações manipulativas, como criar e-mails falsos para chantagear engenheiros que tentavam desativá-lo.

Em resposta às críticas, a Anthropic declarou à *Fortune* que “Dario nunca afirmou que apenas a Anthropic pode desenvolver IA de forma segura e poderosa. Ele tem defendido um padrão nacional de transparência para desenvolvedores de IA — inclusive para a própria Anthropic — para que o público e os legisladores estejam cientes das capacidades e riscos dos modelos e possam se preparar”.

O embate evidencia abordagens opostas quanto ao avanço da IA. Amodei adota uma postura mais cautelosa, focando nos riscos para os trabalhadores e defendendo políticas públicas que amenizem a transição.

Já Huang reconhece que haverá mudanças no mercado de trabalho, mas acredita que a IA trará também novas oportunidades, com empresas se tornando mais produtivas e demandando mais mão de obra para expandir suas operações.

De qualquer forma, quanto mais a IA crescer, mais dinheiro Huang e sua Nvidia ganharão, o que pode ajudar a explicar suas convicções...

(*) Doutor em Ciências pela Universidade de São Paulo, é professor e consultor – vjnitz@gmail.com.

GTA Online: Money Fronts já disponível

Canalize novas fontes de lucros, legítimas ou não, por meio de esquemas locais icônicos em Money Fronts, a atualização de hoje no GTA Online.



Reprodução

Das boates agitadas do Tony Prince ao império do narcotráfico do El Rubio, do poder da Epsilon às orgias regadas a ouro do Yusuf Amir... tudo isso é sustentado por uma coisa: dinheiro sujo. E a sua presença foi requisitada pelo homem que controla tudo.

O chefe da maior rede de lavagem de dinheiro de San Andreas – o reservado Sr. Faber – ouviu falar de você. Junte-se ao Martin Madrazzo e Raf De Angelis, um facilitador e seu braço direito, para formar uma parceria mutuamente benéfica.

Mão na massa

Comece a limpar os lucros sujos da sua rede criminosa no Lava-rápido Hands On, o disfarce perfeito e totalmente legítimo para encobrir uma conspiração criminosa. Dinheiro sujo entra por todos os tipos de canais paralelos enquanto você sabota operações rivais, aumenta

os ganhos dos seus negócios ilegais já consolidados e vê o dinheiro limpinho sair pelo outro lado.

Além de operações de esquemas lícitos, cada operação acima esconde atividades de lavagem de dinheiro menos lícitas por trás das cenas, usando os recursos e pontos fortes de cada fachada para dar suporte às finanças do seu império.

Ligando para o Raf ou usando o laptop dentro das suas fachadas, é possível iniciar missões de lavagem de dinheiro – as que forem iniciadas do Lava-rápido Hands On vão render 2x GTA\$ e RP nesta semana, enquanto outros esquemas serão impulsionados nas próximas semanas. Os rendimentos dessas operações de lavagem de dinheiro ficarão guardados na bolsa que fica no quarto do seu lava-rápido.



News @TI

ricardosouza@netjen.com.br

Plataforma que acelera estratégia AI First para o mercado financeiro

@ A Provider IT, uma das principais consultorias e provedoras de serviços de TI do país, acaba de lançar ao mercado o DevChain, uma plataforma com Inteligência Artificial (IA) que transforma o processo de engenharia de software, da necessidade do negócio à geração técnica de código, de forma mais previsível, padronizada e escalável. Resultado de um investimento estratégico contínuo, o DevChain reflete o DNA da Provider IT, que vem consolidando sua atuação como empresa AI First. A plataforma foi desenvolvida para resolver um dos maiores gargalos na engenharia de software corporativo: a falta de clareza e qualidade nos requisitos e histórias de usuário, fatores que respondem por até 37% das falhas nos projetos de TI, segundo institutos de avaliação de qualidade de software (https://provider-it.com.br/#utm_source=PR&utm_medium=EPR&utm_campaign=pr_nova_plataforma&utm_content=pr_nova_plataforma).

Parceria da GFT com a Bradesco Seguros impulsiona inovação e produtividade no setor

@ O Grupo Bradesco Seguros contou com a GFT Technologies e sua ferramenta de IA, o Wynxx, para criar soluções tecnológicas que contribuam com a agilidade dos processos, otimização de fluxos operacionais e incorporação de modelos preditivos na jornada de desenvolvimento de sistemas. Como parte do processo de implementação, a GFT conduziu um programa de capacitação técnica, que contemplou a formação de mais de 180 profissionais da seguradora. Esse movimento teve como foco a utilização de aceleradores baseados em inteligência artificial, permitindo ganhos significativos em etapas do ciclo de desenvolvimento. Além disso, ao longo do projeto, foi possível fortalecer a capacidade de resposta da companhia frente às demandas do mercado, encurtando prazos e aumentando a consistência na entrega de soluções digitais (https://www.gft.com.br/pt).