



OPINIÃO

O maior risco para os sistemas industriais não é a computação quântica, e sim esperar por ela

Rafael Silva (*)

A integração entre Tecnologia da Informação (IT) e Tecnologia Operacional (OT) trouxe ganhos expressivos em produtividade, automação, monitoramento remoto e eficiência nos ambientes industriais, mas ao mesmo tempo ampliou a superfície de ataque das infraestruturas críticas.

Agora, um novo desafio começa a ganhar espaço entre os líderes de segurança: o impacto da computação quântica sobre a criptografia que protege equipamentos, comunicações e identidades digitais nos ambientes industriais.

O tema costuma ser tratado como um problema do futuro, mas essa percepção pode ser perigosa. Segundo a McKinsey, a computação quântica deixou de ser uma aposta de longo prazo para se tornar uma prioridade estratégica. A consultoria estima que o mercado global de criptografia pós-quântica poderá alcançar US\$ 2.4 - 3.4 bi até 2035.

Esse movimento mostra que a discussão já saiu dos laboratórios e passou a fazer parte do planejamento das grandes organizações. O motivo é simples: criminosos já utilizam a estratégia conhecida como Harvest Now, Decrypt Later, roubando informações criptografadas hoje para descriptografá-las no futuro, quando computadores quânticos forem capazes de romper os algoritmos atuais. Para empresas de energia, manufatura, óleo e gás, saneamento, telecomunicações e transporte, isso significa que projetos industriais, credenciais, certificados digitais e comunicações estratégicas podem já estar sendo armazenados por atacantes.

Nos ambientes de OT, esse cenário é ainda mais preocupante porque a infraestrutura industrial possui um ciclo de vida muito diferente da TI corporativa. Enquanto servidores e aplicações são renovados em poucos anos, controladores industriais (PLCs), sistemas SCADA, sensores, dispositivos embarcados e equipamentos de automação permanecem em operação por uma ou até duas décadas. Muitos deles utilizam algoritmos criptográficos incorporados ao firmware e que, no futuro, não oferecerão mais proteção suficiente. Em diversos casos, a atualização desses sistemas exigirá intervenções presenciais, substituição de equipamentos ou longos processos de certificação.

Esse é justamente o motivo pelo qual a criptografia pós-quântica não deve ser tratada como um projeto tecnológico, mas como um programa estratégico de gestão de riscos. Esperar que a computação quântica se torne uma realidade para só então iniciar a migração significa correr contra o tempo em uma infraestrutura que, por natureza, demora anos para ser modernizada. Nas operações industriais, mudanças são pla-

nejadas cuidadosamente para evitar impactos na produção, tornando a antecipação um fator decisivo para o sucesso da transição.

O primeiro passo dessa jornada é construir um inventário criptográfico completo. Poucas organizações conseguem responder com precisão onde a criptografia está presente em seus ambientes de OT. Certificados digitais, VPNs industriais, autenticação entre equipamentos, assinaturas de firmware, comunicação entre dispositivos e gerenciamento de identidades compõem uma cadeia de confiança extensa e muitas vezes invisível. Sem esse diagnóstico, torna-se impossível avaliar riscos, definir prioridades ou estabelecer um plano consistente de migração para algoritmos resistentes à computação quântica.

Outro ponto que precisa entrar nas discussões estratégicas é a relação com fornecedores. Empresas que adquirem equipamentos industriais hoje deveriam exigir informações claras sobre compatibilidade com criptografia pós-quântica, cronogramas de atualização e capacidade de suportar os novos padrões definidos internacionalmente. Da mesma forma, arquiteturas baseadas no conceito de “crypto agility”, capazes de substituir algoritmos criptográficos sem reconstruir toda a infraestrutura, passarão a representar um importante diferencial para preservar investimentos e reduzir custos futuros.

Também será essencial fortalecer a proteção das chaves criptográficas que sustentam toda a infraestrutura de confiança. Os Hardware Security Modules (HSMs) preparados para suportar algoritmos pós-quânticos oferecem um ambiente seguro para geração, armazenamento e gerenciamento dessas chaves, protegendo certificados, assinaturas digitais e mecanismos de autenticação utilizados nos sistemas industriais. Em infraestruturas críticas, onde uma credencial comprometida pode interromper uma linha de produção ou afetar serviços essenciais à sociedade, proteger as chaves significa proteger toda a operação.

A computação quântica ainda não mudou a indústria. Mas ela já mudou a forma como as organizações precisam pensar sua estratégia de segurança. A pergunta deixou de ser quando os computadores quânticos chegarão e passou a ser quanto tempo sua empresa levará para preparar uma infraestrutura construída para durar décadas. As organizações que iniciarem agora o mapeamento de seus ativos criptográficos, cobrarem preparação de seus fornecedores e incorporarem a criptografia pós-quântica aos seus projetos de modernização estarão muito mais preparadas para enfrentar a próxima grande transformação da cibersegurança. As demais poderão descobrir, tarde demais, que a vulnerabilidade começou muitos anos antes do primeiro ataque quântico.

(*) Diretor da Futuress Brasil.

Hyperscalers

Poder concentrado na nuvem

A revolução digital fez surgir uma nova classe de gigantes invisíveis: os hyperscalers.

Vivaldo José Breternitz (*)

Esse nome é dado a empresas como Amazon Web Services, Microsoft Azure e Google Cloud que operam data centers extremamente grandes, onde são armazenados e processados os dados que permitem a milhões de usuários acessar serviços digitais sem interrupções. São eles que garantem que plataformas de streaming, redes sociais e sistemas bancários funcionem de forma confiável, mesmo em momentos de picos de demanda.

Mas por trás dessa eficiência há um ponto crítico que precisa ser discutido: a concentração de poder. Poucos fornecedores globais controlam a espinha dorsal da economia digital, o que significa que governos, empresas e cidadãos dependem de estruturas privadas para acessar serviços essenciais. A soberania digital, inclusive no Brasil, torna-se uma questão urgente.

Outro desafio é a dependência tecnológica. Ao migrar para a nuvem de um hyperscaler, muitas organizações acabam presas a um ecossistema específico, dificultando a mudança para outro provedor. Essa prática, conhecida como **lock-in**, pode limitar a autonomia das empresas e aumentar custos a longo prazo.

Há ainda o impacto ambiental. Data centers extremamente grandes consomem enormes quantidades de energia e água. Embora os hyperscalers invistam em efi-



4X-image_CANVA

ciência energética e fontes renováveis, o crescimento exponencial da demanda digital levanta dúvidas sobre a sustentabilidade desse modelo.

No Brasil, a presença desses gigantes já é realidade, com diversos deles instalados especialmente no estado de São Paulo. Isso traz benefícios claros, como menor latência, acesso a tecnologias de ponta; empresas de qualquer porte podem usar a mesma infraestrutura, pagando apenas pelos recursos que utilizam. No entanto, a questão que permanece é: quem controla os dados e a infraestrutura crítica que sustentam nossa vida digital?

Em resumo: atualmente os hyperscalers são indispensáveis para o funcionamento da sociedade conectada. Mas é preciso olhar além da eficiência técnica e discutir os riscos de concentração de poder, dependência e impacto ambiental.

O futuro da nuvem não pode ser apenas uma corrida por escala; precisa ser também uma reflexão sobre autonomia, sustentabilidade e equilíbrio entre inovação, segurança e responsabilidade.

(*) Doutor em Ciências pela Universidade de São Paulo, é professor, consultor e diretor do Fórum Brasileiro de Internet das Coisas – vjnit2@gmail.com.

ABIACOM lança fórum para discutir padronização e integridade do e-commerce e marketplaces

AI/ABIACOM



A Associação Brasileira de Inteligência Artificial e E-commerce (ABIACOM) lançou o Fórum de Padronização e Integridade do E-commerce e Marketplaces, iniciativa que pretende reunir representantes da indústria, associações, plataformas digitais, empresas de tecnologia, academia e Poder Público para discutir critérios, padrões técnicos e boas práticas para o comércio eletrônico brasileiro.

O lançamento ocorre em um momento de avanço das discussões sobre a regulação dos marketplaces e a responsabilidade das plataformas digitais. A iniciativa foi apresentada durante o workshop “Marketplaces e Comércio Eletrônico: Novas Fronteiras de Direito e Regulação”, promovido pelo Ministério Público Federal (MPF) e reuniu representantes do Poder Público, empresas como Amazon, OpenAI, TikTok e Mercado Livre, além de pesquisadores e especialistas de instituições como FGV, UNB, IDP, Insper e UFPE.

A ABIACOM participa do debate sobre combate à pirataria e integridade do comércio digital desde 2019, quando passou a colaborar com iniciativas ligadas ao Conselho Nacional de Combate à Pirataria (CNCPI), incluindo a elaboração de materiais de boas práticas e governança.

A criação do Fórum surge como uma evolução dessa atuação. A proposta é estabelecer um espaço permanente e multissetorial para

discutir como o comércio eletrônico e os marketplaces podem adotar padrões capazes de reduzir a circulação de produtos irregulares, falsificados e piratas, além de ampliar a segurança, a transparência e a confiança nas relações digitais.

O tema ganhou ainda mais relevância diante dos impactos econômicos provocados pelo comércio ilícito no país. Levantamentos citados pela ABIACOM apontam perdas de centenas de bilhões de reais para a economia brasileira, considerando prejuízos à indústria e à arrecadação de impostos.

“A ideia é transformar um debate que já existe em uma agenda estruturada, com participação de diferentes setores. Precisamos construir critérios que sejam tecnicamente viáveis, que aumentem a integridade das plataformas e que

contribuam para um ambiente de comércio eletrônico mais seguro para empresas e consumidores”, afirma André Iizuka, vice-presidente da ABIACOM.

A proposta também dialoga com discussões que já vêm sendo realizadas no âmbito do Grupo de Trabalho de E-commerce do Ministério do Desenvolvimento, Indústria, Comércio e Serviços (MDIC). A iniciativa busca contribuir para a construção de uma agenda de padronização e integridade do comércio digital.

O debate sobre o tema foi um dos destaques do workshop do MPF. André Iizuka participou do painel “Combate à contrafação em marketplaces”, com a apresentação sobre “Pirataria no comércio eletrônico e medidas de contenção” (<https://abiacom.org/forum-de-padronizacao/>).

News @ TI

ricardosouza@netjen.com.br

Plano Fácil, agente de IA que coloca informação na palma da mão de mais de 3,6 mil corretores

A inteligência artificial já faz parte de diferentes etapas da jornada de compra de um imóvel, mas, para a Plano&Plano, a tecnologia também pode transformar a rotina de quem está na linha de frente dessa relação. A companhia acaba de lançar o Plano Fácil, agente de inteligência artificial desenvolvido para apoiar exclusivamente os mais de 3,6 mil corretores que integram sua força de vendas. Disponível diretamente pelo WhatsApp, a ferramenta permite consultar informações comerciais em poucos segundos, ampliando a autonomia dos profissionais durante o atendimento aos clientes. O Plano Fácil funciona como um assistente de vendas, capaz de responder dúvidas sobre diferentes etapas da operação comercial. Por meio da assistente de IA Priscila, os corretores podem consultar informações sobre produtos, processos e financiamento imobiliário, incluindo regras de crédito, simulações e enquadramento no Minha Casa, Minha Vida (MCMV) (www.planoefacil.com.br).

TEAM International e Sitecore estreiam operação no Brasil

A TEAM International, empresa americana de desenvolvimento de software e consultoria em tecnologia, oficializa sua chegada ao Brasil declarando o país como pilar central de sua estratégia na América Latina. De acordo com um levantamento da companhia, o mercado brasileiro representa 54% de todo o potencial de negócios que a empresa considera endereçável na região. O investimento viabiliza a criação da TEAM CX, unidade dedicada à experiência digital na América Latina, fruto da parceria com a Sitecore, fornecedora global de plataformas de experiência digital. Com o acordo, a TEAM International passa a ser parceira exclusiva da Sitecore no Brasil, México, Colômbia e Argentina, ampliando sua atuação na região. “Essa parceria reforça nossa capacidade de apoiar empresas em projetos de transformação digital e amplia o acesso à tecnologia da Sitecore para organizações na América Latina”, afirma Matt Moore, CEO e presidente do conselho da TEAM International (<https://www.teamcx.com/>).