OPINIÃO

A chegada definitiva da computação quântica está mais perto do que pensamos, assim como seus riscos

Dean Coclin (*)

Em 2015, a McKinsey & Company, uma consultoria de gestão global, publicou um estudo sobre iniciativas de diferentes nações ao redor do mundo em pesquisa e desenvolvimento de tecnologias de computação quântica. Dos 20 países listados, o Brasil ocupava a última posição em volume de capital investido no segmento: sua média anual foi estimada, em valores da época, em R$ 44 milhões.

Embora último, o levantamento tenha sido um grande sinal sobre a produção de conhecimento nacional em computação quântica, na edição mais recente do seu estudo "The Quantum Technology Monitor", divulgado em setembro de 2021, o Brasil nem é mais mencionado pela McKinsey.

Isto é apenas um dos retratos de uma realidade que há anos afeta as pesquisas científicas no país. Os cortes no orçamento público e nos investimentos nas áreas de ciência e tecnologia nos últimos anos têm dificultado a produção de conhecimento por instituições de ensino e pesquisadores brasileiros.

A computação quântica tem uma promessa incrível para o planeta – e o poder de destruir a segurança fundamental da Internet.

Se você acompanha as conversas sobre quantum, provavelmente já ouviu falar do Q-Day – o dia não especificado, mas inevitável, em que os computadores quânticos serão capazes de quebrar os algoritmos de criptografia nos quais confiamos atualmente para proteger a Internet e uma série de processos digitais.

Proponho redefinir o termo para significar o momento em que você precisa estar muito preocupado com a criptoagilidade necessária para preparar sua organização para os riscos da computação quântica.

O ponto de ruptura está mais perto do que você pensa

O "S" em HTTPS (também conhecido como cadeado em seu navegador) é fornecido por um protocolo de criptografia chamado Transport Layer Security (TLS). O TLS usa um esquema de criptografia chamado criptografia assimétrica que depende de um par de chaves: uma chave pública que criptografa dados e verifica assinaturas digitais e uma chave privada que descriptografa dados e gera assinaturas digitais. Os algoritmos assimétricos mais comuns hoje são RSA e ECC.

Usamos criptografia assimétrica para proteger as comunicações de rede, como quando você insere as informações do seu cartão de crédito ou identificação de contribuinte em um site. Também usamos criptografia assimétrica para proteger outras chaves de criptografia (encapsulamento de chaves), como aquelas usadas para proteger bancos de dados massivos em nuvens e data centers em todo o mundo. Simplificando, a criptografia assimétrica atualmente protege praticamente tudo.

A criptografia assimétrica usa matemática complexa (grandes números primos) que é muito difícil de ser resolvida pelos supercomputadores atuais. Mas a computação quântica é excepcional na resolução de problemas matemáticos complexos. E em algum momento, os computadores quânticos terão energia suficiente para resolver rapidamente o complexo problema matemático que é a criptografia assimétrica.

O mais importante não é quando, mas como

Ninguém sabe exatamente quando isso vai acontecer, mas o "quando" não é o ponto. O que deveríamos nos preocupar – muito preocupados – é quanto tempo levará para atualizar todos os nossos sistemas para serem quânticos seguros. E eu quero dizer tudo: todos nossos sistemas, como prontuários médicos, bombas de gasolina, caixas eletrônicos, serviços públicos, comunicações militares…

Isso não significa que tudo o que foi protegido com criptografia RSA será exposto imediatamente ou simultaneamente. Em vez disso, significa que qualquer chave privada pode ser derivada rapidamente (pense em horas, não em dias), tornando mais fácil para os invasores falsificarem ou explorarem os itens protegidos sempre que desejarem.

Tornando o quantum seguro

RSA e ECC são de uso muito geral. Nós os usamos para criptografar e descriptografar informações e gerar assinaturas digitais para verificar a autenticidade das mensagens. Esse não é o caso dos atuais algoritmos de criptografia pós-quântica (PQC). O que significa que casos de uso específico exigirão algoritmos diferentes.

Vinte e oito algoritmos PQC estão atualmente em desenvolvimento, quatro dos quais o NIST (Instituto Nacional de Padrões e Tecnologia) propôs como padrões:

- **Crystals-Kyber** para encapsulamento de chave de criptografia (ML-KEM)
- **Cristais-Dilithium** para assinaturas digitais (ML-DSA)
- **SPHINCS+** para assinaturas digitais (SLH-DSA)
- **FALCON** para assinaturas digitais (FN-DSA)

Em relação aos recursos computacionais, por exemplo, as assinaturas digitais criadas usando RSA 2048 têm 256 bytes, enquanto as assinaturas digitais criadas usando SPHINCS+ têm 17 kilobytes (66 vezes maiores).

Você deve ter notado que o NIST está considerando três algoritmos de assinatura digital para padrões. Cada um tem vantagens distintas que são úteis para diferentes casos de uso. O dilítio é preferível para assinatura quântica segura de uso geral. SPHINCS+ deve ser usado para casos de uso de alta segurança. O FALCON oferece verificação rápida de assinaturas, tornando-o ideal para aplicações de IoT de nicho.

O que você deve fazer para começar a se preparar hoje

A prontidão quântica não é algo que sua empresa possa alcançar em um dia e não existe uma solução única. As organizações mais protegidas serão criptoágeis, permitindo-lhes substituir ativos criptográficos desatualizados sem interromper a infraestrutura do seu sistema.

Alcançar a criptoagilidade começa com:

- Criando um inventário de seus certificados, algoritmos e outros ativos criptográficos
- Trocar algoritmos de criptografia por: raízes de confiança (por exemplo, autoridades de certificação privadas da sua organização), firmware para dispositivos de longa duração e quaisquer outros ativos que produzam assinaturas que precisam ser confiáveis por um longo tempo; e

Explorando maneiras de incorporar algoritmos quânticos seguros em seus produtos Colocando em prática a cripto-agilidade

A modernização da infraestrutura de segurança cibernética mundial para que seja quântica segura não será rápida e provavelmente exigirá várias tentativas. O PQC está em desenvolvimento há muitos anos, mas é lógico que as primeiras versões aprovadas para uso podem não resistir ao teste do tempo.

Além do mais, os algoritmos PQC não são um substituto igual para os algoritmos em uso hoje. Teremos que suportar mais algoritmos, e os tamanhos das chaves e o texto cifrado resultante (dados criptografados) exigirão mais recursos computacionais do que os algoritmos atuais.

O Q-Day não é apenas hoje; é todos os dias daqui em diante. É por isso que o verdadeiro objetivo é a agilidade criptográfica, com ênfase na "agilidade". A verdadeira prontidão quântica significa estar preparado para se adaptar rapidamente às mudanças e ter soluções de segurança implementadas que permitam a adaptação sem causar grandes interrupções em seus negócios.

(*) É desenvolvimento de negócios sênior da DigiCert.

Inteligência artificial protegendo operadores de call centers

É notório que os operadores de call centers têm um trabalho desagradável, estressante.

Vivaldo José Breternitz (*)

MART_PRODUCTION_de_PEXELS_CANVA

Durante todo o expediente atendem clientes insatisfeitos, muitas vezes grosseiros, agressivos e só podem responder usando o jargão corporativo obrigatório, formal.

Provavelmente a inteligência artificial virá a substituir esses profissionais, mas enquanto isso não acontece, várias empresas estão usando inteligência artificial para lidar com o sofrimento emocional dos funcionários de seus call centers.

Recentemente, o enorme conglomerado japonês SoftBank anunciou que até o início de 2026 implantará uma tecnologia que vem chamando de "cancelamento de emoção" que usará inteligência artificial para proteger seus funcionários, noticiou o jornal Asahi Shimbun.

Essa tecnologia, chamada SoftVoice, transformará as vozes irritadas de clientes em vozes mais calmas, agindo como um "escudo mental" para os operadores.

Os desenvolvedores do SoftVoice disseram ao jornal japonês que a inteligência artificial detectará tons de voz hostis e automaticamente alterará a inflexão dos clientes, sem mudar suas palavras.

O SoftBank não está sozinho nesse esforço; o banco americano First Horizon, com sede em Memphis, está usando inteligência artificial para detectar quando um operador de call center está prestes a perder a paciência e nesse momento envia ao mesmo um vídeo mostrando fotos de sua família, com música suave ao fundo e instruções sobre técnicas de respiração relaxante.

Os funcionários desse banco escolhem as fotos e músicas que aparecerão em seus vídeos, que duram um minuto. Com o uso dessa tecnologia, o First Horizon diz ter registrado uma redução de 20% nos níveis de burnout de seus três mil operadores de call center.

Apesar de serem ações positivas, um usuário da plataforma Reddit fez uma observação muito pertinente acerca do assunto: "Esta é a pior solução possível – lembrei-me de quando trabalhadores da Apple na China começaram a se suicidar devido às condições de trabalho, jogando-se das janelas. A "solução" encontrada foi colocar redes nas mesmas, sem procurar sanar as causas dos problemas"...

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

Cnco dicas para começar a empreender digitalmente

Freepik

Segundo a edição 2023/2024 do relatório Global Entrepreneurship Monitor, principal pesquisa sobre empreendedorismo do mundo, o Brasil é o país que tem o maior percentual de donos de empresas que têm a expectativa de ampliar o uso de tecnologias digitais para vender seus produtos ou serviços nos próximos 6 meses. Entre empresas em estágio inicial de desenvolvimento, ou early-stage, o índice chega a 90%.

Entre as opções de tecnologias digitais, a criação de um site para lançar produtos e serviços online é fundamental. Começar essa jornada como principiante, no entanto, pode ser desafiador. Por isso, separamos cinco dicas do especialista Rafael Hertel, country manager da Hostinger no Brasil, para ajudar você com iniciativas que ajudem nos primeiros passos do seu projeto:

1 - Estabeleça um MVP

Vivemos em um mundo em constante transformação, por isso a maioria das nossas decisões não têm um caráter definitivo e podem mudar. Por outro lado, é necessário que haja rapidez nos negócios. Nesse contexto, é ideal pensar no MVP (Produto Mínimo Viável), que é a versão mais simples necessária para lançar um projeto.

2 - Acompanhe empresas e pessoas do seu nicho que estão onde você quer chegar

Procure as marcas que conquistaram presença digital no mesmo nicho que o seu e analise seus sites, redes sociais e os meios que usam para estabelecer e manter o relacionamento com clientes. Avalie como é a experiência de uso do site, onde e como são feitas as campanhas digitais e os benefícios oferecidos online.

3 - Tenha paciência, resiliência e confiança no processo

Na internet, as coisas acontecem de forma repentina, depois de um processo de lenta evolução. No início, pode parecer que os esforços estão sendo em vão, mas é importante seguir porque há um momento em que tudo muda. Isso acontece porque o trabalho na internet é exponencial. Por isso, os resultados, quando chegam, podem ser inimagináveis.

4 - Escolha um nome cativante para seu projeto e registre um domínio condizente

A definição do domínio de um site é fundamental para refletir adequadamente o seu negócio online. Para escolher o nome, é preciso levar em conta que os visitantes precisam memorizá-lo para acessar seu site. Uma boa opção atual para ajudar na escolha é a inteligência artificial. Se ainda não tem marca, esse tipo de ferramenta pode, ainda, ajudar a criá-la, inclusive com logo.

5 - Escolha o melhor CMS (plataforma gerenciadora de conteúdos) e publique seu site

Hoje, o acesso à criação de um site está disponível para pessoas que não tenham conhecimento de programação e que podem lançar o seu negócio online de maneira rápida e fácil. Com o criador de sites de Hostinger, por exemplo, é possível criar um site apenas digitando três frases para a inteligência artificial ou editar "arrastando e soltando" elementos preestabelecidos.

News @TI

ricardosouza@netjen.com.br

MV abre mais de 50 vagas para o setor de tecnologia

@A MV, multinacional brasileira líder da América Latina no desenvolvimento de softwares para a saúde, aceita candidaturas de todo o Brasil para mais de 50 vagas do setor de tecnologia. Há oportunidades para a sede, em Recife (PE), e para as unidades de São Paulo (SP), Fortaleza (CE), Teresina (PI), Blumenau e Brusque (SC). Todas as vagas também são direcionadas a pessoas com deficiência. Dentre as vagas abertas, a MV busca profissionais em arquitetura de soluções, desenvolvimento, analista de infraestrutura, DBA, analista de suporte, consultoria e gerente de projetos. Também há vagas para analista fiscal, analista de negócios, executivos de contas, entre outros. As oportunidades abrangem diversos níveis de carreira. Informações sobre requisitos necessários, detalhes das oportunidades e inscrição podem ser encontrados no portal de carreiras do ecossistema MV (https://prd-pc1.lg.com.br/vagas/c/14E91D1E-3320-4B26-84F9-F5C0345F5B12/p/PortalCarreirasMV/pt-BR/Busca/Index).

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.