A Microsoft tocou em engenheiros da China para suporte ao SharePoint - A

Data: 2025-09-05 22:30:19

Autor: Inteligência Against Invaders

Uma nova investigação revelou que a Microsoft contou com os engenheiros da China para fornecer suporte técnico e correções de bugs para o SharePoint, o mesmo software de colaboração que foi recentemente explorado por hackers chineses patrocinados pelo Estado em um enorme ataque cibernético que afeta centenas de organizações, incluindo agências governamentais sensíveis dos EUA.

No mês passado, Microsoft anunciado O fato de os hackers chineses exploraram com sucesso as vulnerabilidades no SharePoint para violar os sistemas de computadores de inúmeras empresas e agências governamentais, incluindo a Administração Nacional de Segurança Nuclear e o Departamento de Segurança Interna.

No entanto, o que a empresa não divulgou em seu anúncio foi que o suporte do SharePoint foi tratado por uma equipe de engenharia da China há anos.

De acordo com as capturas de tela internas do sistema de rastreamento de trabalho da Microsoft revisadas pela ProPublica, os funcionários da China estavam recentemente consertando bugs para o SharePoint “Onprem”-a versão local do software que foi direcionada nos ataques do mês passado.

Esta versão refere -se ao software instalado e operado nos próprios computadores e servidores dos clientes, tornando -o particularmente vulnerável à manipulação direta.

Quando confrontado sobre esse acordo, a Microsoft defendeu suas práticas, afirmando que a equipe da China “é supervisionada por um engenheiro dos EUA e sujeita a todos os requisitos de segurança e revisão do código do gerente”.

A empresa também anunciou que “o trabalho já está em andamento para mudar este trabalho para outro local”, embora nenhuma linha do tempo específica tenha sido fornecida.

Embora ainda não esteja claro se a equipe da Microsoft, sediada na China, desempenhou algum papel no SharePoint Hack, especialistas em segurança cibernética alertaram consistentemente sobre os riscos significativos de segurança representados ao permitir que o pessoal chinês realizasse suporte e manutenção técnica nos sistemas governamentais dos EUA.

O padrão mais amplo de preocupação

Essa revelação faz parte de um padrão maior que surgiu em relação à dependência da Microsoft em trabalhadores estrangeiros. A investigação da ProPublica constatou que, por mais de uma década, a Microsoft depende de trabalhadores estrangeiros – incluindo aqueles com sede na China – para manter os sistemas em nuvem do Departamento de Defesa.

A supervisão desses trabalhadores estrangeiros vem de pessoal baseado nos EUA, conhecido como “acompanhantes digitais”, que geralmente não têm a experiência técnica avançada necessária para monitorar efetivamente seus colegas estrangeiros.

O acordo de escolta foi originalmente desenvolvido pela Microsoft para satisfazer funcionários do Departamento de Defesa que estavam preocupados com funcionários estrangeiros e atender aos requisitos de que as pessoas que lidam com dados sensíveis são cidadãos dos EUA ou residentes permanentes.

Apesar dessas medidas, o sistema deixou informações altamente sensíveis vulneráveis ??devido à diferença de habilidade técnica entre acompanhantes e os engenheiros estrangeiros que supervisionam.

As revelações levaram uma resposta significativa do governo. O secretário de Defesa Pete Hegseth lançou uma revisão abrangente da confiança das empresas de tecnologia em engenheiros estrangeiros para apoiar o departamento.

Além disso, os senadores Tom Cotton (R-Arkansas) e Jeanne Shaheen (D-New Hampshire) escreveram várias cartas para a Hegseth, citando a investigação da ProPublica e exigindo informações mais detalhadas sobre as operações de suporte baseadas na Microsoft.

Em resposta à pressão crescente, a Microsoft anunciou que havia interrompido o uso de engenheiros da China para apoiar o Departamento de Defesa Computação em nuvem sistemas e estava pensando em implementar a mesma mudança para outros clientes do governo em nuvem.

O momento dessas revelações é particularmente preocupante, dado o escopo do recente ataque do SharePoint. A análise da Microsoft mostrou que os hackers chineses começaram a explorar as fraquezas do SharePoint em 7 de julho de 2025.

A empresa lançou um patch inicial em 8 de julho, mas os hackers o ignoraram com sucesso, forçando a Microsoft a emitir um patch mais robusto com proteções aprimoradas.

A agência de segurança de segurança cibernética e infraestrutura dos EUA alertou que essas vulnerabilidades permitem que os hackers “acessem totalmente o conteúdo do SharePoint, incluindo sistemas de arquivos e configurações internas, e executem código pela rede”.

Os ataques também foram usados ??para se espalhar Ransomwareque criptografa os arquivos das vítimas e exige pagamento por sua liberação.

Impacto e implicações futuras

As agências governamentais relataram níveis variados de impacto da violação. O Departamento de Segurança Interna declarou que não há evidências de que os dados foram retirados da agência, enquanto o Departamento de Energia, que supervisiona a Administração Nacional de Segurança Nuclear, descreveu o impacto como “mínimo” sem informações sensíveis ou classificadas.

Olhando para o futuro, a Microsoft anunciou que, a partir de julho próximo, não suportará mais versões locais do SharePoint, pedindo aos clientes que migrassem para a versão online.

Essa transição se alinha à estratégia de negócios mais ampla da Microsoft de promover serviços baseados em assinatura e sua plataforma de computação em nuvem do Azure, que contribuiu significativamente para o recente marco de avaliação da empresa de se tornar a segunda empresa da história a exceder US $ 4 trilhões em valor de mercado.

Esta investigação levanta questões fundamentais sobre os protocolos de segurança que envolvem a infraestrutura crítica de software e os riscos potenciais de acordos internacionais de pessoal em um cenário cada vez mais complexo de segurança cibernética.

Encontre esta história interessante! Siga -nos LinkedIn**e**X**Para obter mais atualizações instantâneas**.