Paralisação do governo dos EUA para reduzir a equipe federal de seguran

Data: 2025-10-02 16:30:00

Autor: Inteligência Against Invaders

A paralisação do governo dos EUA esgotará severamente os recursos federais de segurança

cibernética, com a Agência de Segurança Cibernética e Infraestrutura (CISA) prestes a perder cerca

de 65% de sua força de trabalho.

Estima-se que 1651 funcionários da CISA de sua força de trabalho de 2540 funcionários devem ser dispensados, deixando apenas 889 restantes no cargo, de acordo com um Departamento de Segurança Interna (DHS) oficial Documento de planejamento publicado antes do desligamento.

Isso apesar do DHS esperar reter 91% de sua força de trabalho total durante a paralisação.

A CISA, que opera sob o DHS, é responsável pela proteção da segurança cibernética em todos os níveis do governo federal. Além disso, fornece orientação e compartilhamento de inteligência de ameaças com estados, setor privado e parceiros internacionais.

Isso inclui financiamento e apoio para o Vulnerabilidades e exposições comuns (CVE) , uma referência para vulnerabilidades divulgadas publicamente.

Nenhum detalhe foi fornecido sobre os tipos de funções que serão dispensadas.

Além disso, o site da CISA não será gerenciado ativamente até que um acordo seja alcançado sobre um orçamento no Senado dos EUA, permitindo que o financiamento federal seja retomado.

Um notar no site diz: “Este site foi atualizado pela última vez em 30 de setembro de 2025 e não será atualizado até que o financiamento seja promulgado. Como tal, as informações neste site podem não estar atualizadas. As transações enviadas por meio deste site podem não ser processadas e não poderemos responder às perguntas até que as dotações sejam promulgadas.

A CISA não é a única agência cibernética a ser afetada. O Departamento de Comércio estima em seu plano de desligamento que o Instituto Nacional de Padrões e Tecnologia (NIST) manterá apenas 34% de sua força de trabalho.

O NIST desenvolve uma gama de Padrões e estruturas de segurança cibernética, que são usados globalmente pelas organizações para ajudar a proteger suas redes.

Isso inclui o NIST Cybersecurity Framework (CSF) e Padrões de criptografia pós-quântica.

Como CISA, NIST’s local na rede Internet atualmente traz um aviso de que não está sendo

atualizado devido a um “lapso nas dotações anuais”.

O desligamento traz graves riscos cibernéticos

A perspectiva de que as atividades da CISA e do NIST sejam reduzidas levantou temores de que os cibercriminosos possam explorar falhas críticas de segurança para lançar ataques.

Isso inclui a capacidade do governo de responder a ataques em suas redes, como corrigir vulnerabilidades críticas.

Outra questão é que as agências federais podem ser forçadas a suspender contratos com fornecedores terceirizados, incluindo aqueles que fornecem serviços de segurança cibernética ao governo.

Além disso, as empresas e autoridades locais dos EUA não receberão as notificações e recomendações usuais da CISA e do NIST, incluindo alertas sobre novos tipos de ameaças e explorações de vulnerabilidade.

Brandon Potter, CTO da ProCircular, alertou que tanto os cibercriminosos motivados financeiramente quanto os atores do estado-nação provavelmente aumentarão os ataques para explorar a situação.

“Espere ver um aumento nos ataques de ransomware direcionados a fornecedores de infraestrutura crítica durante esse período; no entanto, eles provavelmente mudarão apenas para exfiltração e extorsão de dados para amplificar ainda mais as tensões políticas”, comentou.

“É um jogo longo com persistência baixa e lenta. Se eu sou um ator de ameaças de estado-nação com uma posição razoável na rede, meu objetivo seria continuar uma penetração mais profunda e estabelecer várias formas de persistência para aumentar a longevidade e o sucesso da missão”, acrescentou Potter.

Os especialistas também preveem que os funcionários federais em licença serão alvo de vários ataques de fraude e engenharia social.

“A oportunidade de riscos de exploração aumentará em relação ao phishing que visa credenciais. Especialmente aqueles que visam trabalhadores em licença devido ao número de logins e sites esporádicos nos quais trabalharão para comunicações oficiais de RH e benefícios. Espere ataques coordenados contra contas de e-mail pessoais e de trabalho desses trabalhadores”, observou Potter.

O impacto da segurança cibernética nos EUA provavelmente durará muito além do período de paralisação, comentou Gary Barlet, CTO do setor público da Illumio.

“Quando o desligamento termina, a TI não simplesmente liga novamente. O trabalho se acumulou e desacelerou, os projetos em andamento ou apenas começando foram paralisados e as pausas no financiamento foram interrompidasf linhas do tempo. Esses atrasos afetam os esforços cibernéticos e de TI planejados”, disse Barlet.

Os projetos de segurança cibernética de longo prazo provavelmente serão deixados de lado, pois a equipe estará sob pressão para priorizar correções imediatas.

Quanto tempo pode durar a paralisação do governo?

A paralisação entrou em vigor à meia-noite EST de quarta-feira, 1º de outubro, depois que o partido republicano do presidente Donald Trump não conseguiu aprovar um projeto de lei de gastos que financia serviços governamentais após uma disputa com representantes democratas no Senado.

Em um Coletiva de imprensa em 1º de outubro, a secretária de imprensa da Casa Branca, Karoline Leavitt, alertou que os funcionários federais poderiam ser demitidos em dois dias.

O Escritório de Orçamento do Congresso (CBO) estima que 750.000 funcionários federais serão dispensados no total.

Não está claro quanto tempo a paralisação pode durar. O recorde atual de 35 dias, de dezembro de 2018 a janeiro de 2019, ocorreu durante o primeiro mandato do presidente Trump.

Os funcionários em licença enfrentarão licença sem vencimento, mas terão direito a pagamentos retroativos assim que o orçamento para os gastos do governo for aprovado.