A lei cibernética dos EUA expirada coloca em risco o compartilhamento de

Data: 2025-10-03 01:19:56

Autor: Inteligência Against Invaders

Uma lei crítica dos EUA que protege as empresas de responsabilidade legal ao compartilhar

inteligência de ameaças cibernéticas expirou depois que os legisladores não conseguiram chegar a

um acordo durante um impasse de financiamento do governo.

A Lei de Compartilhamento de Informações de Segurança Cibernética de 2015 (CISA 2015) protegeu as empresas de ações judiciais ao trocar dados de ameaças cibernéticas por meio de um programa voluntário chamado Programa Automatizado de Compartilhamento de Indicadores (AIS).

Esperava-se que a lei expirasse em 30 de setembro, a menos que o Congresso dos EUA votasse para estendê-la antes dessa data.

Apesar do apoio bipartidário e dos avisos urgentes dos líderes do setor, os legisladores permitiram que a lei caducasse, deixando as empresas expostas a possíveis ações judiciais e enfraquecendo uma defesa importante contra ataques cibernéticos.

Saiba mais sobre a Lei de Compartilhamento de Informações de Segurança Cibernética: Porto Seguro da CISA 2015 em Risco à medida que o prazo de setembro de 2025 se aproxima

Agora, com uma paralisação do governo desencadeada pelo fracasso do Congresso em aprovar o projeto de lei de financiamento, a extensão da lei permanece incerta.

Lapso da CISA 2015: uma crise de segurança nacional em formação

Muitos profissionais de segurança cibernética estão profundamente preocupados com o fato de que o lapso da CISA 2015 pode ter consequências de longo alcance nas defesas cibernéticas dos EUA.

Saša Zdjelar é o Chief Trust Officer da ReversingLabs, uma empresa que dependia fortemente da lei para manter repositórios de ameaças robustos.

Ele disse que esse lapso é “um caso clássico de disfunção política criando vulnerabilidades reais”.

“Na ReversingLabs, vimos em primeira mão como a lei permite o tipo de compartilhamento robusto de inteligência de ameaças que mantém as defesas atualizadas. Tire essas proteções, e a defesa coletiva que nos manteve fortes por uma década começa a desmoronar, dando aos adversários uma vantagem que eles não merecem”, acrescentou.

Além disso, Zdjelar espera que esse episódio provavelmente coloque em risco o compartilhamento de inteligência de ameaças e aumente a ameaça de vulnerabilidades da cadeia de suprimentos de software.

Ele também argumentou que o lapso poderia ter “um efeito assustador” no desenvolvimento da segurança da IA.

“A incerteza jurídica forçará as empresas a se tornarem conservadoras sobre o compartilhamento de dados de ameaças necessários para treinar ferramentas de segurança baseadas em IA, dificultando o desenvolvimento de defesas contra ataques habilitados por IA”, explicou.

Andy Lunsford, CEO da empresa de resposta a incidentes BreachRx, chamou o fracasso em renovar a CISA 2015 de “uma crise em formação.”

Ele alertou que alguns de seus clientes – já sobrecarregados pela escassez de talentos, multas regulatórias mais severas e aumento dos custos de detecção e escalonamento – “ficarão escuros” no compartilhamento de ameaças sem proteções legais, criando pontos cegos perigosos na defesa cibernética.

“Os números mais recentes da IBM [from the *2025 IBM Cost of a Data Breach Report*] mostrar que os EUA são o marco zero para violações de dados; eles são mais caros aqui do que em qualquer outro lugar do mundo por uma ampla margem. Sem a CISA 2015, espero que esses números dobrem em escala e custo dentro de um ano”, acrescentou.