Entenda falha no sistema da CrowdStrike que causou apagão cibernético

Uma falha na atualização de conteúdo relacionada ao sensor de segurança CrowdStrike Falcon, que serve para detectar possíveis invasões de hackers, foi a causa do ataque cibernético desta sexta-feira (19), que deixou milhares de empresas e pessoas em todo o mundo sem acesso a sistemas operacionais, especialmente o Windows, da Microsoft.

A empresa de segurança cibernética Crowdstrike, responsável pelo apagão, foi categórica ao afirmar que o incidente de hoje não foi um ataque. O que de fato aconteceu na madrugada desta sexta-feira, de acordo com a empresa, foi uma atualização de conteúdo para os arquivos hosts Windows da Microsoft.

Um arquivo Host é usado pelo sistema operacional no mapeamento de hosts amigáveis para endereços IP (Protocolo de Internet) numéricos que identificam e localizam um outro host em uma rede IP. Esses arquivos host contém linhas de texto que são endereços de IP e eles se comunicam.

O CrowdStrike Falcon que foi atualizado e acabou dando problema é um sensor que pode ser instalado justamente nos sistemas operacionais Windows, da Microsoft, Mac ou Linux. São módulos de produtos que se conectam a um ambiente de soluções de segurança chamados de endpoint, que é hospedado na nuvem. Esse sensor permite acesso instantâneo às informações de “quem, quando, onde e como” ocorreu um ataque, e sua arquitetura criada em nuvem permite períodos de resposta e correção rápidos e precisos.

Um endpoint security, ou ponto final de segurança, oferece proteção para os dispositivos. A computação em nuvem é o fornecimento de serviços de computação, incluindo servidores, armazenamento, banco de dados, rede, software, análise e inteligência, pela internet (a nuvem), oferecendo inovações rápidas com recursos flexíveis e economias de escala. E foram esses serviços que apresentaram dificuldades de acesso a plataformas de empresas em todo o mundo.

De acordo com a Lei Geral de Proteção de Dados (LGDP), a segurança de endpoint trabalha para garantir a proteção das informações sensíveis, e ajuda a empresa a cumprir as regras de proteção de dados. Isso quer dizer que há uma necessidade crescente de medidas de segurança que as empresas devem ter para evitar ameaças cibernéticas.

Mitigação

Mais cedo, a Microsoft informou que medidas de mitigação estavam sendo adotadas, mas alertou que muitos usuários poderiam não conseguir acessar vários aplicativos e serviços, como ocorreu ao redor do mundo. As empresas afetadas acabaram identificando que utilizam o sistema de segurança da CrowdStrike

Por causa da situação ocorrida hoje, as ações da empresa, cotadas na abertura do mercado acionário a US$ 351 dólares, eram negociadas na tarde desta sexta-feira a US$ 297, uma queda de mais de US$ 50, o que significou uma perda de valor de mercado da CrowdStrike superior a US$ 2 bilhões em um único dia.

Ataques rastreados

O site da empresa CrowdStrike informa, em seu Relatório Global de Ameaças, tendências e eventos notáveis em todo o cenário de ciberameaças, que detectou 34 adversários recém-identificados em 2023. Mais de 230 ataques adversários no total foram rastreados pela empresa, e as intrusões na nuvem, onde ocorreu o problema verificado hoje, aumentaram em 75%.

Segundo a empresa, o tempo para comprometimento de e-crime mais rápido registrado foi de dois minutos e sete segundos. O relatório também apontou que o aumento de vítimas de roubo de dados identificados na dark web foi de 76%. O relatório de inteligência examina como os adversários estão operando e constata-se uma furtividade sem precedentes, com adaptação dos ataques rápidos para evitar a descoberta pelos sistemas de segurança.

Agência Brasil