

E agora, como se resolve? A boa e a má notícia sobre a falha informática

 eco.sapo.pt/2024/07/19/e-agora-como-se-resolve-a-boa-e-a-ma-noticia-sobre-a-falha-informatica

Ironicamente, uma atualização de cibersegurança derrubou sistemas em todo o mundo e lançou a confusão. A solução requer intervenção direta em cada máquina, mas não exige conhecimentos muito avançados.

A falha informática que está a gerar caos a nível mundial esta sexta-feira teve origem numa atualização de um programa informático da CrowdStrike, **usado por muitas empresas para protegerem os seus sistemas, incluindo computadores usados pelos trabalhadores, mas também servidores**. O erro na atualização provocou um conflito com o sistema operativo Microsoft Windows, o mais usado em todo o mundo, deixando milhares de equipamentos inoperacionais.

Ao início da manhã desta sexta-feira começaram a surgir relatos de constrangimentos num conjunto alargado de serviços nos quatro cantos do planeta, começando pela Austrália e chegando a localizações tão distantes como EUA, Índia e Europa. As companhias aéreas estiveram entre as empresas mais afetadas, mas o problema também derrubou emissões de televisão e caixas de hipermercados. Em Portugal, a ANA, gestora dos aeroportos nacionais, não foi “diretamente” afetada, mas **alertou os passageiros para possíveis constrangimentos devido a problemas em algumas das empresas que operam nas suas infraestruturas**.

Segundo especialistas ouvidos pelo ECO, a CrowdStrike é uma empresa de cibersegurança norte-americana e um dos maiores fornecedores mundiais deste tipo de *softwares*, chamados Endpoint Detection and Response Solutions (EDR). **A empresa lançou uma atualização durante a madrugada que provocou um erro fatal nos equipamentos Windows com esse programa instalado**. Esse erro é vulgarmente conhecido por *blue screen of death* (BSOD), ou só *blue screen*, e pode acontecer por inúmeros motivos. Ainda está por explicar porque é que um erro na atualização da CrowdStrike interferiu de uma forma tão fundamental com todo o sistema operativo dos equipamentos afetados.

“Há uma falha num **software bastante vulgarizado entre as grandes empresas, que, na interação com o Windows, causa um erro**. As pessoas estão a associar o problema à Microsoft, mas só quem tem [o programa da] CrowdStrike é que tem problemas”, explica ao ECO o especialista em cibersegurança Rodrigo Adão da Fonseca. Em causa está “uma ferramenta de cibersegurança colocada nos chamados *endpoints* — telemóveis, tablets, servidores — e que, se está dispersa e a atualização é feita de forma automática”, gera de imediato um “problema de disponibilidade”, acrescenta.

Nem todas as empresas clientes da CrowdStrike com sistemas Windows tiveram problemas. O ECO ouviu de uma fonte bem posicionada no setor que **houve empresas em Portugal que conseguiram escapar ao problema por testarem todas as atualizações fornecidas por terceiros antes de as distribuírem**, de forma geral, pelos seus equipamentos.

Há uma falha num software bastante vulgarizado entre as grandes empresas, que, na interação com o Windows, causa um erro.

Rodrigo Adão da Fonseca
Especialista em cibersegurança

A boa e a má notícia

Quanto tempo vai demorar a resolver o problema? É impossível prever, pois vai depender de cada empresa, mas há uma boa e uma má notícia. **A má é que não será possível reverter automaticamente o problema nas máquinas afetadas**, pois os sistemas estão totalmente indisponíveis e sem acesso à internet. Ou seja, vai ser preciso intervir diretamente em cada máquina, com permissões de administração, segundo os especialistas.

A boa é que a CrowdStrike **está a propor como solução aos clientes um processo que requer poucos conhecimentos técnicos para implementar, apurou o ECO**. É necessário reiniciar o computador, entrar num modo específico do Windows (modo de segurança) e apagar o ficheiro que estará a provocar o conflito. Segundo um especialista, “um técnico de primeira linha consegue resolver”.

Na rede social X, o CEO da CrowdStrike, George Kurtz, confirmou a existência de um problema que afeta só os sistemas Windows — “Mac e Linux não são impactados” — e **garantiu que não se trata “de um incidente de segurança ou um ciberataque”**. “O problema foi identificado, isolado e foi feita uma correção”, disse, acrescentando: “A nossa equipa está toda mobilizada para garantir a segurança e estabilidade dos clientes da CrowdStrike.”

| [Tweet from @George_Kurtz](#)

Todas as fontes ouvidas e consultadas pelo ECO são unânimes na opinião de que este problema vai deixar a CrowdStrike em maus lençóis. **“A CrowdStrike deixou de ser uma empresa confiável”, desabafou com o ECO uma pessoa que está a lidar diretamente com a situação**. Já o CEO da empresa de cibersegurança VisionWare, Bruno Castro, comenta que “ninguém esperaria isto vindo de um fabricante destes”, destacando que a CrowdStrike era conhecida por ter “um ADN muito grande de confidencialidade, integridade e disponibilidade”. Antes da abertura das bolsas nos EUA, as ações da CrowdStrike chegaram a cair 21% na manhã desta sexta-feira, um sinal claro do nervosismo dos investidores.

"Temos um mega fabricante que, ao colocar os sistemas indisponíveis, causa um efeito dominó que coloca em causa o ciberespaço todo."

Bruno Castro
CEO da Visionware

O que nos diz este problema sobre a forma como o mundo funciona atualmente? **“Diz-nos uma coisa muito importante: estamos cada vez mais dependentes do mundo cibernético.** Temos um mega fabricante que, ao colocar os sistemas indisponíveis, causa um efeito dominó que coloca em causa o ciberespaço todo”, afirma Bruno Castro, CEO da VisionWare.

Por sua vez, Rodrigo Adão da Fonseca diz que **é preciso “olhar com alguma normalidade para estes problemas, a partir do momento em que somos mais digitais”.** “Temos as vantagens, mas também temos de perceber que há falhas. É resolver, assumir a chatice. É a parte má de todas as vantagens que o mundo digital nos traz.”

A questão é que quem perdeu negócio por causa deste problema, quem ficou em terra porque o avião não descolou ou quem sofreu danos reputacionais porque o serviço esteve indisponível poderá não querer deixar passar isto em branco. A imprensa internacional reportou problemas nos aeroportos de Mumbai a Madrid e no transporte ferroviário no Reino Unido. A cadeia televisiva *Sky News* ficou impedida de fazer a emissão em direto. **Quando a poeira assentar, muitas destas empresas vão exigir mais explicações... mas também responsabilidades.**