Apagão: Hipótese de ciberataque está quase descartada. Mas ainda há dúvidas que persistem

tek.sapo.pt/noticias/internet/artigos/apagao-hipotese-de-ciberataque-esta-quase-descartada-mas-ainda-ha-duvidas-que-persistem

5 de maio de 2025

Uma semana depois de **um apagão que é descrito como uma das maiores falhas do sistema elétrico na Europa** e que, em Portugal, deixou milhões de pessoas sem eletricidade durante cerca de 10 horas, **a causa do incidente ainda está a ser investigada, mas a possibilidade de um ciberataque, inicialmente considerada, está agora quase afastada**.

Num primeiro momento, Manuel Castro Almeida, Ministro Adjunto e da Coesão Territorial, admitiu que o apagão poderia ter sido causado por um ciberataque. "Há essa possibilidade, mas não está confirmada", respondeu em declarações à RTP 3. Com **a falta de confirmação acerca do que se estava a passar, as dúvidas continuaram a avolumar-se e, com os rumores que circulavam online, ganharam outra dimensão**.

Nas redes sociais e em apps de mensagens como o WhatsApp corria informação falsa de que o apagão se devia a um ciberataque russo, numa suposta confirmação por parte de Ursula Von der Leyen, ou até de que a CNN Internacional tinha avançado com uma notícia nesse sentido, como noticiou o Polígrafo.

Mas, poucas horas depois do início do apagão, começaram a chegar as primeiras indicações de que a falha na rede elétrica não teria sido causada por um ataque informático. Em Portugal, **o Centro Nacional de Cibersegurança (CNCS) anunciou que, até ao momento, não existiam indícios que apontassem para um ciberataque**, alertando também para a circulação de informação falsa acerca do sucedido.

Teresa Ribera, vice-presidente executiva da Comissão Europeia, avançou que não existiam para já provas de ciberataque no corte maciço no abastecimento elétrico na Península Ibérica, uma **informação corroborada também pela Agência Europeia para a Segurança das Redes e da Informação (ENISA)**.

Em declarações à Bloomberg, um porta-voz agência europeia afirmou que, embora o caso estivesse a ser cuidadosamente analisado, **as primeiras investigações mais para uma falha técnica do que para um ataque informático**.

No dia a seguir ao apagão, **a Red Elétrica de Espanha (REE), empresa que gere a rede elétrica do país, descartou a hipótese de um ciberataque na origem do incidente**. Porém, o Tribunal Nacional Espanhol iniciou uma investigação preliminar para apurar se essa possibilidade podia ser realmente descartada.

Um ciberataque poderia causar um apagão?

Embora a hipótese de um ciberataque esteja, para já, quase descartada pelas autoridades competentes, **o caso levanta questões importantes. Por exemplo: poderia um ataque informático causar um apagão em grande escala como o que aconteceu em Portugal e Espanha?**

fonte oficial do CNCS começa por reforçar que, "no contexto do acompanhamento da falha na rede elétrica nacional", tem estado "em estreita cooperação com as autoridades nacionais e com congéneres europeus desde a ocorrência do incidente, **não havendo, até ao momento, evidências que o identifiquem como tendo origem num ciberataque"**.

A entidade realça que "**existe uma comunicação permanente entre o CNCS e os operadores de infraestruturas críticas**, que passa pela partilha de conhecimento e de indicadores de cibersegurança, nomeadamente através da divulgação de situações de ameaças, vulnerabilidades e incidentes, que visam melhorar a ciber-resiliência do setor energético".

No que toca aos tipos de ataques que têm maior potencial de causar disrupções a larga escala na rede elétrica nacional, **o CNCS explica que "o impacto de potenciais ciberataques na rede elétrica alargada depende do vetor de ataque à rede e suas interligações"**.

"Ainda assim, e face à experiência de alguns congéneres, tais como a Ucrânia, **consideramos o malware com caráter destrutivo, vulgarmente designado por wipers, uma tipologia de ataque com um impacto mais prejudicial para qualquer rede mista IT/OT**, pelo grau de dificuldade quanto à recuperação dos dados", detalha.

As infraestruturas críticas têm se tornado cada vez mais num alvo para cibercriminosos, em particular, daqueles que são apoiados por Estados-NaçãoCheck Point Software lembra, por exemplo, o caso de um ataque na Ucrânia que, em 2015, deixou os habitantes de Kiev sem eletricidade. Neste caso, o ataque foi atribuído à unidade de inteligência cibermilitar russa, conhecida como Sandworm.

Bruno Castro, CEO da VisionWare e especialista em Cibersegurança e Análise Forense, aponta também para o mesmo caso ucraniano, realçando que, dado às suas características, **os sistemas de gestão das redes elétricas modernas são vulneráveis a ciberataques se não forem devidamente protegidos.**

O responsável detalha que além de malware, como aconteceu no caso da Ucrânia em 2015, **existem vários vetores de ataque que podem ser usados por cibercriminosos para tentar comprometer o funcionamento de infraestruturas críticas** como uma rede energética.

Aqui contam-se, por exemplo, **campanhas de Spear Phishing** para roubar dados sensíveis e aceder aos sistemas, assim como a **exploração de vulnerabilidades** em ambientes industriais, sem esquecer **ataques a empresas terceiras que tenham ligações às operadoras da rede**.

As consequências do ataque dependeriam dos obejtivos do mesmo, indica a Check Point Software. **"Se for um ataque disruptivo, o mais provável será simplesmente paralisar o sistema e evitar ao máximo o seu restauro"**. No entanto, num caso em que não houvesse energia elétrica nem telecomunicações, "será sempre muito difícil que esse ataque seja algo dinâmico".

"No caso dos ataques por ransonware, em que o objetivo do mesmo é o da exfiltração de dados para a criação de um posterior pedido de resgate, estes tendem a não afetar o funcionamento do serviço durante esse processo, para não levantarem suspeitas junto dos operadores de sistemas", detalha a empresa de cibersegurança.

Rumores vindos da Dark Web e redes sociais

Ainda na semana passada, a Iniciativa CpC: Cidadãos pela Cibersegurança deu conta de **anúncio na Dark Web que oferecia acesso a infraestrutura crítica no México, publicado poucas horas após o incidente europeu**. Embora indique que não existem dados públicos que confirmem essa ligação direta, a Iniciativa afirma que “a hipótese não pode ser descartada sem investigação forense”.

Além de um anúncio na Dark Web, a CpC aponta também dá também conta que dois grupos de cibercriminosos com afiliação pró-Rússia, **Dark Storm Team e NoName057(16)**, terão **reivindicado publicamente**, através da rede social X e Telegram, **a responsabilidade pelo apagão**.

Ao SAPO TEK, o CNCS indica que, “através do CERT.PT, **detetou e analisou as alegadas reivindicações feitas por parte dos grupos Dark Storm Team e NoName057(16)**, que detêm um historial de ataques ao longo do último ano, quase sempre de negação de serviço, tipologia improvável de ter causado o incidente que provocou a falha elétrica”. **“O CNCS ainda não exclui, até ao momento, qualquer causa para a falha no fornecimento de energia”**, realça a entidade.

Já do lado da VisionWare, Bruno Castro afirma que **“neste momento, não existem evidências técnicas concretas que estabeleçam uma ligação direta entre o anúncio identificado e o apagão que afetou Portugal e Espanha”**. “Embora a proximidade temporal possa levantar hipóteses de correlação, **é essencial salientar que correlação não implica causalidade**”, afirma.

O responsável indica que o cenário é complexo, o “que requer uma **análise forense aprofundada e a cooperação entre entidades nacionais e internacionais para confirmação de qualquer ligação**”. “Será por isso prematuro tirar ilações nesta fase”, afirma.

Embora a equipa da VisionWare não tenha detetado “qualquer anúncio diretamente relacionado com entidades portuguesas ou espanholas que possa ser claramente associado ao apagão”, a empresa verificou que **“vários fóruns e canais no Telegram aumentaram a sua atividade, com menções indiretas ao evento, o que é muito comum após incidentes com esta carga e visibilidade mediática”**.

No que toca aos grupos Dark Storm Team e NoName057(16), o responsável afirma que a Visionware tem conhecimento das alegadas reivindicações, que "estão a ser analisadas também no contexto mais amplo da sua atividade conhecida". Segundo Bruno Castro, **os dois grupos têm um "histórico de campanhas de desinformação e de reivindicação oportunista de incidentes de grande impacto, mesmo quando não têm qualquer envolvimento direto".**

Na visão do CEO da VisionWare, **a hipótese mais plausível é que as revindicações destes grupos tenham apenas como objetivo "amplificar a percepção de poder e causar instabilidade"**, aproveitando a cobertura mediática do incidente. "Naturalmente, todas as possibilidades continuam a ser consideradas em sede de investigação, mas até ao momento, não existem provas técnicas que confirmem a autoria destes incidentes por parte destes referidos grupos", realça.

Preparar para o pior cenário

Em caso de **confirmação de ciberataque, que procedimentos é que os operadores responsáveis pela gestão e distribuição de eletricidade em Portugal teriam de seguir?** Embora a Diretiva NIS2, que traz novas obrigações para as empresas, ainda esteja em processo de transposição para o contexto nacional, o CNCS afirma que **"o atual Regime Jurídico da Segurança do Ciberespaço determina que os operadores de infraestruturas críticas adotem medidas previstas na nova diretiva europeia"**.

Entre elas contam-se **medidas relativas à "notificação de incidentes com impacto relevante ou substancial**", mas também as que dizem respeito à **realização de análises dos riscos "em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que tais operadores utilizam"** e a implementação de **medidas de segurança adequadas**, como previsto no Regime Jurídico da Segurança do Ciberespaço e no Quadro Nacional de Referência de Cibersegurança.

A entidade lembra que os **operadores de infraestruturas críticas devem também adotar medidas de governação e comunicação ao CNCS**, que envolvem a designação de pontos de contacto permanentes e de responsáveis segurança, mantendo igualmente inventários e listas de ativos essenciais e elaborando planos de segurança e de relatórios anuais atualizados, que têm de ser enviados ao CNCS.

Já Bruno Castro sublinha que, "dado o aumento da sofisticação dos ciberataques e a crescente dependência de sistemas digitais na gestão de infraestruturas críticas, **é fundamental que as entidades responsáveis pela rede elétrica implementem medidas robustas de cibersegurança**", acrescentando que incidentes como o apagão também servem **"como um forte alerta para o reforço da ciberresiliência no setor energético"**.