Bloco de Esquerda

ASSEMBLEIA DA REPÚBLICA

	Expeça - se
☐ **REQUERIMENTO** Número / (.ª)	**Publique - se**
☒ **PERGUNTA** Número 73 / XVII (2 .ª)	2026-10-01
	O Secretário da Mesa German a Rocha (Assinatura Qualificada) Assinado por: Germana Rocha (Assinatura Qualificada) Data: 01/10/2026 11:39:21 +01:00

Assunto: Ciberataque à Universidade de Aveiro, exploração de vulnerabilidades críticas nos produtos de VPN da Check Point Software Technologies utilizados por instituições públicas de ensino superior e silêncio institucional perante a comunidade académica

Destinatário:Ministro da Educação, Ciência e Inovação

Exmo. Senhor Presidente da Assembleia da República

A 9 de março de 2026, o Bloco de Esquerda tornou público que a Universidade de Aveiro (UA) assenta o seu serviço de rede privada virtual (VPN) em tecnologia da Check Point Software Technologies, empresa com sede em Telavive. O serviço de teletrabalho da UA, gerido pelos Serviços de Tecnologias de Informação e Comunicação (sTIC), impõe aos utilizadores, em todos os sistemas operativos, o cliente Capsule/Endpoint Security da Check Point, que apenas estabelece ligação a um Security Gateway do mesmo fabricante. Páginas públicas de configuração mostram que a mesma solução é usada na Universidade do Porto (FEUP, FCUP, ICBAS e FFUP) e na Universidade NOVA de Lisboa (FCSH). Contactada pela agência Lusa, a UA escusou-se a reagir. Não se conhece, até hoje, qualquer esclarecimento da instituição sobre a arquitetura do serviço, sobre onde termina o túnel VPN, sobre quem tem acesso técnico ao tráfego ou sobre a avaliação de impacto que uma escolha desta natureza exige.

A 29 de julho de 2026, a UA informou que detetara um acesso indevido aos seus sistemas de informação, do qual resultou a exposição de dados pessoais e institucionais. O Reitor explicou à Lusa e à Renascença que o ataque acontecera «há uns dias», que a instituição só se apercebeu da sua extensão na tarde de 28 de julho, quando foi contactada por correio eletrónico pelos próprios atacantes, os quais apresentaram prova da informação copiada e pretendiam chegar a um «acordo justo».

A 30 de julho, o Centro Nacional de Cibersegurança (CNCS) precisou que o CERT.PT fora notificado a 20 de julho, que se tratou de um ataque de ransomware com exfiltração de informação de caixas de correio eletrónico e de, pelo menos, uma base de dados, que o incidente foi participado à Polícia Judiciária e à Comissão Nacional de Proteção de Dados (CNPD), e que o CERT.PT solicitou à UA os elementos necessários à análise e recomendou medidas adicionais de reforço da segurança. Toda a comunidade académica, 13.626 estudantes de graduação, 3.811 de pós-graduação, cerca de 1.400 docentes e investigadores e 650 trabalhadores técnicos, administrativos e de gestão, foi obrigada a alterar a palavra-passe.

Desde 30 de julho não há informação pública nova. Não se sabe que base de dados foi exfiltrada, que categorias de dados contém, quantas pessoas são afetadas, se os dados

foram publicados, se houve negociação com os atacantes, qual foi o vetor de entrada, nem se foi realizada uma auditoria forense independente.

O incidente da UA ocorreu no meio de uma sequência de vulnerabilidades críticas, exploradas ativamente, nos produtos da Check Point que suportam serviços de VPN:

A 8 de junho de 2026, a Check Point publicou um aviso de segurança sobre a CVE-2026-50751 (CVSS 9.3), um contorno de autenticação nas soluções Remote Access VPN e Mobile Access configuradas com o protocolo IKEv1, que permite a um atacante remoto estabelecer uma sessão de VPN sem palavra-passe válida. A própria empresa datou de 7 de maio a primeira exploração observada, referiu um aumento das tentativas no início de junho, identificou «algumas dezenas» de organizações visadas em todo o mundo e confirmou, num dos casos, atividade pós-compromisso associada a um afiliado do ransomware Qilin. No mesmo dia, o CNCS emitiu o alerta correspondente (CVE-2026-50751 / EUVD-2026-35047), listando entre as versões afetadas várias já fora de suporte.

A 23 de julho de 2026, três dias depois da notificação do CERT.PT sobre a UA, a Check Point registou ataques dirigidos, de dia zero, contra a CVE-2026-93616 (CVSS 9.8), vulnerabilidade de execução de código sem autenticação no Security Management; a 27 de julho, o CNCS publicou um alerta de vulnerabilidade relativo ao Check Point Security Management.

A 9 de setembro de 2026, a Check Point corrigiu as CVE-2026-85102 e CVE-2026-85103 (ambas CVSS 9.8), que permitem execução remota de código sem autenticação no tratamento de certificados durante a negociação VPN nos Security Gateways, incluindo em configurações de Remote Access VPN. A partir de 12 de setembro observou-se uma vaga de tentativas de exploração, o NCSC dos Países Baixos alertou a 10 de setembro, a CERT-EU emitiu o aviso 2026-012 e, a 22 de setembro, a agência norte-americana CISA incluiu as falhas no seu catálogo de vulnerabilidades exploradas, com prazo de correção até 25 de setembro e a indicação de que qualquer equipamento exposto deve ser tratado como potencialmente já comprometido e sujeito a triagem forense.

Não é a primeira vez: em maio de 2024, a CVE-2024-24919, nos mesmos gateways com Remote Access VPN, foi explorada e motivou alertas da CERT-EU e do CNCS.

O Bloco não afirma que qualquer destas vulnerabilidades tenha sido o vetor do ataque à UA: a instituição não o revelou. Mas uma universidade que assenta o seu perímetro de segurança num produto atingido por três vagas de exploração ativa em cinco meses, e que sofre um ataque de ransomware com exfiltração nesse mesmo intervalo, deve à sua comunidade e à tutela uma resposta clara sobre as versões instaladas, as datas de aplicação das correções e os resultados das análises forenses.

A Check Point Software Technologies foi fundada em 1993 por Gil Shwed, Marius Nacht e Shlomo Kramer. Shwed desenvolveu a tecnologia nuclear da empresa enquanto servia na Unidade 8200, o principal serviço de inteligência de sinais das Forças Armadas de Israel, e preside hoje ao seu conselho de administração, o atual diretor executivo, Nadav Zafrir, é antigo comandante da mesma Unidade 8200.

A empresa integra, com a Israel Aerospace Industries, um dos principais fabricantes de armamento de Israel, os consórcios IC3 (2016) e IAC3 (2018). Em novembro de 2024, o Ministério da Defesa turco confirmou ao parlamento daquele país que as suas forças armadas tinham abandonado os produtos Check Point desde 2016. Estas ligações não são um pormenor biográfico: são a razão pela qual a escolha deste fornecedor para a infraestrutura crítica de acesso remoto de instituições públicas de ensino superior exige uma avaliação de impacto e uma decisão fundamentada, e não uma mera adjudicação técnica.

O tratamento de dados de tráfego de rede de dezenas de milhares de pessoas por infraestrutura de um fornecedor externo, e a exfiltração de caixas de correio e bases de dados, convocam diretamente o Regulamento (UE) 2016/679 (RGPD): o princípio da

integridade e confidencialidade (artigo 5.º, n.º 1, alínea f)), a obrigação de segurança do tratamento (artigo 32.º), a notificação de violações à CNPD no prazo de 72 horas após o conhecimento (artigo 33.º), a comunicação aos titulares quando o risco é elevado (artigo 34.º), a avaliação de impacto sobre a proteção de dados (artigo 35.º) e o regime das transferências para países terceiros (artigos 44.º a 49.º), sendo que a decisão de adequação relativa a Israel (Decisão 2011/61/UE, reafirmada pela Comissão Europeia em 2024) não cobre o acesso por serviços de informação ou forças armadas, como resulta da jurisprudência Schrems II (processo C-311/18). Convocam ainda a Diretiva (UE) 2022/2555 (NIS 2), que inclui as organizações de investigação entre as entidades importantes, e as orientações e medidas mínimas de cibersegurança do CNCS para as entidades públicas. A UA é uma fundação pública com regime de direito privado sob tutela do Ministério da Educação, Ciência e Inovação, e a autonomia universitária não dispensa a tutela de conhecer e de agir.

Chegaram ao Bloco de Esquerda relatos de membros da comunidade académica da UA segundo os quais, após o ataque, a rede da Universidade registou recentemente falhas frequentes e estando praticamente inoperacional em vários dias, em pleno arranque do ano letivo, sem que a instituição tenha explicado à comunidade a origem dos problemas, a sua relação com o incidente ou as medidas em curso. O silêncio de março repete-se em setembro.

Assim, ao abrigo das disposições constitucionais e regimentais aplicáveis, a Representação Parlamentar do Bloco de Esquerda vem perguntar ao Governo, através do Ministério Ministério da Educação, Ciência e Inovação, o seguinte:

1. Quando e por que via tomou o Ministério conhecimento do ciberataque à Universidade de Aveiro, e que informação recebeu da instituição desde então?

2. Qual foi o vetor de entrada do ataque? Envolveu o Security Gateway da Check Point que suporta o serviço de VPN da UA, ou qualquer outro equipamento deste fabricante? Se o vetor não foi apurado, foi realizada auditoria forense independente e com que conclusões?

3. Que versão e que correções (jumbo hotfix takes) estavam instaladas nos equipamentos Check Point da UA a 7 de maio, a 8 de junho, a 20 de julho e a 9 de setembro de 2026? O protocolo IKEv1 estava ativo no serviço de acesso remoto? Em que datas foram aplicadas as correções relativas às CVE-2026-50751, CVE-2026-93616, CVE-2026-85102 e CVE-2026-85103?

4. A UA cumpriu os alertas do CNCS de 8 de junho e de 27 de julho de 2026 e as recomendações adicionais do CERT.PT? Foi feita a triagem forense recomendada pelas autoridades internacionais para os equipamentos expostos?

5. Que base de dados foi exfiltrada, que categorias de dados pessoais contém e quantas pessoas são afetadas? Os dados exfiltrados foram publicados ou colocados à venda? Os atacantes foram identificados?

6. Houve contactos ou negociação com os atacantes na sequência do pedido de «acordo justo»? Foi pago ou ponderado o pagamento de qualquer resgate? Qual é a orientação do Governo para as instituições públicas de ensino superior quanto ao pagamento de resgates, tendo em conta que o CNCS integra a iniciativa No More Ransom?

7. Em que data tomou a UA conhecimento da violação de dados, em que data notificou a CNPD nos termos do artigo 33.º do RGPD, e em que data e por que meio comunicou a violação aos titulares afetados nos termos do artigo 34.º? Como se explica o intervalo entre a notificação do CERT.PT, a 20 de julho, e a informação à comunidade, a 29 de julho?

8. Foi realizada avaliação de impacto sobre a proteção de dados (artigo 35.º do RGPD) relativa ao serviço de VPN e à infraestrutura de segurança de perímetro da UA,

designadamente após a denúncia pública de março? Com que conclusões?

9. Onde termina o túnel VPN dos utilizadores da UA: em equipamento instalado e operado pela Universidade, ou em infraestrutura em nuvem operada pela Check Point ou por terceiros? Que entidades têm acesso técnico, ainda que potencial, ao tráfego, aos registos de ligação e aos metadados dos utilizadores, e em que jurisdição?

10. Quando, por que procedimento, por que valor e através de que fornecedor ou revendedor foi contratada a solução Check Point da UA, e quando termina ou se renova o contrato? Foram ponderadas alternativas europeias ou de código aberto auditável?

11. A UA ou o Ministério consultaram a CNPD ou o CNCS sobre a utilização desta solução? Existe, no Ministério, inventário das instituições de ensino superior público que utilizam produtos Check Point em serviços de VPN ou de segurança de perímetro?

12. A instabilidade da rede da UA em agosto e em setembro está relacionada com o incidente de julho, com os trabalhos de remediação ou com novas tentativas de intrusão? Que serviços foram afetados e por quanto tempo? Que impacto teve no arranque do ano letivo?

13. Por que razão a UA não prestou qualquer informação pública desde 30 de julho? Foi apresentado relatório ao Conselho Geral da Universidade? Que apoio foi dado às pessoas cujas caixas de correio foram copiadas, designadamente face ao risco de fraude e de phishing dirigido?

14. Que orientações transmitiu ou vai transmitir o Ministério às instituições de ensino superior público, designadamente à Universidade do Porto e à Universidade NOVA de Lisboa, para a aplicação urgente das correções da Check Point e para a análise de eventuais compromissos anteriores, nos termos recomendados pelo CNCS, pela CERT-EU e pela CISA?

15. Considera o Governo compatível com a Estratégia Nacional de Segurança do Ciberespaço, com a Diretiva NIS 2 e com os objetivos de soberania digital da União Europeia que infraestruturas críticas de rede de universidades públicas dependam de um único fornecedor extraeuropeu, de código fechado, com ligações estruturais aos serviços de inteligência militar de um Estado terceiro, e cujos produtos foram objeto de três vagas de exploração ativa em cinco meses?

16. Que critérios de responsabilidade em matéria de direitos humanos e de direito internacional tenciona o Ministério promover nos procedimentos de contratação tecnológica das instituições sob a sua tutela, à luz das ligações documentadas deste fornecedor ao complexo militar e de inteligência israelita?

Palácio de São Bento, 30 de Setembro de 2026

Deputado(a)s

ANDREIA GALVÃO(BE)

Nos termos do Despacho n.º 1/XIII, de 29 de outubro de 2015, do Presidente da Assembleia da República, publicado no DAR, II S-E, n.º 1, de 30 de outubro de 2015, a competência para dar seguimento aos requerimentos e perguntas dos Deputados, ao abrigo do artigo 4.º do RAR, está delegada nos Vice-Presidentes da Assembleia da República.