Nº 2142 | 22 abril 2022

O Jornal Económico

| Diretor Filipe Alves | Subdiretores André Cabrita-Mendes, Ligia Simões, Nuno Vinha e Ricardo Santos Ferreira | Diretor de Arte Mário Malhão | Preço €3,50 (continente) | Semanário, sai às sextas-feiras

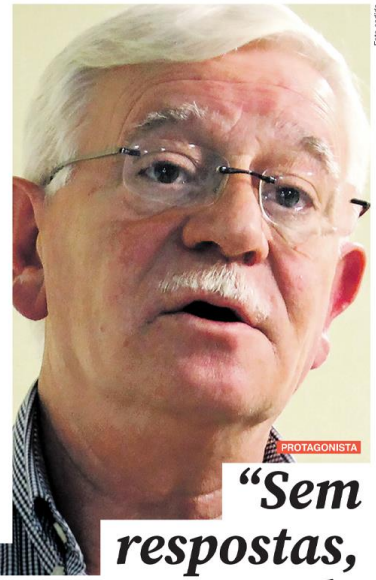

Foto cedida

PROTAGONISTA

"Sem respostas, pode haver um crescendo de agitação social"

A proposta de Orçamento do Estado traz muito pouco para os trabalhadores da Administração Pública. Se não houver respostas, poderá haver um crescendo de desconforto. O aviso é deixado por José Abraão, secretário-geral da Federação dos Sindicatos da Administração Pública (FESAP). ■ P4

OE2022

Proposta sem surpresas em matérias fiscal replica, no essencial, versão chumbada

Análise às medidas fiscais dirigidas às empresas e famílias, previstas no Orçamento do Estado de "contas certas". Leia a opinião da EY e consulte as simulações com os novos escalões do IRS. ■ Especial OE

FRANÇA

Abstenção passou a ser o principal adversário de Macron nas presidenciais de domingo ■ P12

Emmanuel Macron
Candidato presidencial pela La République En Marche!

COM O SEU JORNAL ECONÓMICO

Não perca os especiais Banca Online e Trading e Escolas de Gestão: Pós Graduações ■ Suplementos

Clara Raposo
Presidente do ISEG

Mansão dos Espírito Santo com 22 quartos à venda por 16 milhões de euros

Sociedade dona do emblemático palacete – uma moradia com 1.820 m2 de área construída, 45 divisões e 22 quartos – é detida pelos herdeiros da mãe de Ricardo Salgado, incluindo o ex-banqueiro. Família já tinha feito uma tentativa de venda em 2019, mas o processo falhou porque o ex-presidente do BES tinha os bens arrestados por ordem do tribunal. ■ P19

Taxa contra precariedade arrisca ser novamente adiada

O Governo anunciou que iria cobrar em 2023 a taxa que penaliza as empresas com contratos a prazo "em excesso". Falhou, porém, a publicação dos diplomas necessários para que medida chegue ao terreno, abrindo a porta a novo adiamento. ■ P6

BANCA

Novobanco exige quatro milhões de euros em juros de mora devido a atrasos na tranche de 2021

Em causa está verba retida pelo ministro João Leão. Ramalho e equipa acumulam cinco milhões em prémios desde 2019. ■ P16

JUSTIÇA

Álvaro Sobrinho ainda sem 'luz verde' para pagar caução de seis milhões com quatro casas

Advogado diz que "ainda não há despacho" do juiz Carlos Alexandre para validar o pedido de pagar a caução com imóveis. ■ P3

CONFERÊNCIA

Empresas têm de aceitar o risco cibernético, mas garantir resiliência e apostar na formação

Conferência organizada pelo JE reuniu especialistas para debater desafios e soluções para a cibersegurança em Portugal. ■ P22

CONFERÊNCIA

Empresas têm de aceitar o risco cibernético, mas garantir resiliência e apostar na formação

Conferência organizada pelo JE reuniu especialistas para debater desafios e soluções para a cibersegurança em Portugal. ■ P22

António Gameiro Marques, Gabinete Nacional de Segurança; Nélson Ferreira, AIG; Paulo Figueiredo, Banco BiG; Teresa Rosas, Fidelidade; Mariana Bandeira, Jornal Económico

Simão de Sant'Ana, Abreu Advogados; Jorge Cadeireiro, Nuc Nogueira, VisionWare; Nuno Vinha, Jornal Económico

uno Nogueira, Decunify; Diogo Pata, Watchguard; Filipe

Da esquerda para a direita: Pedro Latoeiro, Center for Cooperation in Cyberspace, Nuno Teodoro, Huawei Portugal, Timóteo Menezes, Edisoft, David Grave, Claranet Portugal, e António Pinto, BDO; Ricardo Santos Ferreira, Jornal Económico

Fotos: Margarida Cruzeiro e Catarina

CONFERÊNCIA

Empresas têm de aceitar o ciber-risco ou arriscam-se "a viver numa gruta"

A cibersegurança foi o tema central do fórum organizado pelo Jornal Económico, que reuniu líderes e especialistas para entender como vai ser gerido o risco cibernético nas organizações. É necessária formação e resiliência aos ataques.

INÊS AMADO, JOÃO SANTOS COSTA E RODOLFO ALEXANDRE REIS
iamado@jornaleconomico.pt

A indústria da cibersegurança em Portugal vale pelo menos 130 milhões de euros, de acordo com uma estimativa relativa a 2020 avançada por António Gameiro Marques, diretor-geral do Gabinete Nacional de Segurança (GNS) no primeiro Fórum Cibersegurança organizado pelo Jornal Económico (JE) no dia 19 de abril. Na conferência – que juntou no ISEG líderes e especialistas numa discussão sobre a gestão do risco cibernético – o responsável indicou que a entidade que dirige prepara-se para divulgar este e outros dados no mais recente observatório sobre a economia de segurança. No ano passado, 44 mil pessoas receberam certificação do GNS, sendo a aposta na formação o caminho a seguir para uma gestão mais eficaz do risco cibernético, de acordo com Gameiro Marques.

Por outro lado, as alterações legislativas relacionadas com a cibersegurança terão um acrescido impacto no dia-a-dia das organizações e exigirão das mesmas um maior nível de investimento, mas também de responsabilização, acautelou Ricardo Henriques, sócio da Abreu Advogados. O advogado, que arrancou a iniciativa, começou por recordar os ciberataques dos últimos meses.

Ricardo Henriques apontou a "falta de competências de resposta por parte das empresas e a falta de literacia" tanto dos utilizadores, como dos clientes.

O percurso entre o enquadramento atual e as leis que ainda não estão em prática obrigará, segundo o advogado, a um processo de adaptação por parte das organizações, em especial as do sector financeiro, cujos desafios foram abordados no primeiro painel do fórum, moderado pela jornalista do JE Mariana Bandeira.

"As organizações não estão todas no mesmo patamar de consciência e de preparação", diz a Head of IT da Fidelidade, Teresa Rosas

Sector financeiro é um sector apetecível a ataques

As empresas que foram alvo de ataques informáticos no último ano e que estavam bem preparadas para essas ameaças "recuperaram num tempo relativamente curto e recuperaram tudo", explicou o diretor-geral do Gabinete Nacional de Segurança, António Gameiro Marques. O contra-almirante dá como exemplos os ataques à Vodafone e à Sonae que, em situações distintas, conseguiram evitar danos e perturbações maiores devido aos elevados níveis de preparação. "As [empresas] que não estão [preparadas] levam muito tempo e perdem coisas no caminho", alertou o mesmo responsável. Apostar em fatores de autenticação e realizar regularmente ações de formação para os trabalhadores estão entre o conjunto de ações efetivas que, apesar de não protegerem completamente, ressalvou Gameiro Marques, são de adoção premente dada a ameaça crescente que estes sectores enfrentam.

Por sua vez, Teresa Rosas, Head of IT da Fidelidade, deixou clara a importância de se debater diariamente a cibersegurança: "As organizações não estão todas no mesmo patamar de consciência e de preparação", disse, sublinhando que o sector financeiro é um sector apetecível, incorrendo em riscos que outros sectores ainda não enfrentam. "Temos de deixar de pensar que estamos seguros para estarmos preparados. A preparação tem de ser definida por cada organização de acordo com o seu ponto de partida e modelo de negócio", continuou.

Paulo Figueiredo, CTO do Banco Big, também integrou o primeiro painel e foi igualmente categórico quanto à importância da cibersegurança no seio das organizações. "Há uma obrigatoriedade de encarar a segurança como um fator existencial nas organizações. É necessário ter a humildade de sabermos que, por muitas certificações que se tenha, existe sempre um fator de risco por controlar", sublinhou, aludindo à importância de ser mantido internamente uma "postura não só reativa, como proativa".

Já Nelson Ferreira, Portugal Branch Manager e Head of Financial Lines da AIG, abordou a cultura de risco em Portugal para a sociedade, empresários e Governo. "Uma coisa é termos consciência do risco em tempo de crise. Mas a forma de gestão desse risco é diferente se já estiver a ser preparada antes", alertou. Nelson Ferreira defendeu que o debate deve ser alargado ao cidadão e não ficar circunscrito aos especialistas e governantes.

Especialistas pedem mais formação para evitar ataques

A formação e literacia digital são a principal solução para as empresas prevenirem futuros ataques informáticos: "A maioria das pessoas, por desconhecimento ou não, têm sistemas de *wi-fi* que não são seguros ou, ao dividirem casa com terceiros, podem ter acesso a essa informação e assim terem uma porta de entrada para a sua empresa", defendeu Simão de Sant'Ana, advogado-do principal da Abreu Advogados.

Por sua vez, Jorge Cadeireiro, administrador da Nucasc, realçou que 40% dos ataques têm origem no mau comportamento de um funcionário. "Estamos a falar de um colaborador que de forma inadvertida clicou num *link* que não devia", referiu.

Nuno Nogueira, diretor executivo de Tecnologia da Decunify, alertou para o facto de não existir, na esmagadora maioria das empresas portuguesas, um responsável de segurança (um CISO, ou *Chief Information Security Officer*): "Ainda não estamos muito especializados nessa área".

Por outro lado, Diogo Pata, Global Sales Engineer da Watchguard, defendeu a necessidade de uma maior filtragem dos utilizadores e colaboradores. "Existem muitos clientes que ainda estão numa fase de antivírus e *firewall* e que pensam estar protegidos. Qualquer utilizador é um alvo de ataque. É preciso garantir que aquele utilizador é realmente quem diz ser", alertou. Por seu turno, Filipe Custódio, Partner da VisionWave, empresa que oferece soluções de *cloud* integradas para gestão financeira, não tem dúvidas que os ataques informáticos vão continuar. "Não é uma questão de se, mas uma questão de quando vai acontecer", salientou, alertando que não acredita numa distinção entre *hackers* bons e *hackers* maus, dado que o *hacking* é uma atividade tão criminosa como grafitar uma parede. "Olhamos para um *grafiti* e podemos achar que está bem feito, mas numa propriedade privada é crime. No *hacking* é a mesma coisa. Há *hackers* que têm um grande conjunto de *skills* e vão utilizar isso no mercado negro que é onde lhes dá mais dinheiro", sublinhou no painel moderado pelo subdiretor do JE Nuno Vinha.

A cibersegurança está na agenda mundial e empresarial, mas ainda não teve "tradução efetiva e normativa", diz o fundador do Center for Cooperation in Cyberspace, Pedro Latoeiro

"É necessário um empurrãozinho"

Já a forma como as organizações portuguesas vão lidar com o risco foi o tema do painel de encerramento, moderado pelo subdiretor do JE, Ricardo Santos Ferreira. A resposta não passa por ignorar o problema: "Temos que aceitar o risco (...) ou vamos viver para uma gruta, ou numa sociedade digital".

Quem o diz é o diretor da área de Risco Tecnológico e Cibersegurança da BDO, António Pinto. "Acima de tudo, as organizações devem definir o seu apetite e tolerância ao risco", explicou. "Risco zero é impossível. O apetite ao risco tem de ser realista". O Cybersecurity Director da Claranet Portugal, David Grave, não olha à dimensão do país mas ao seu ritmo: "Portugal funciona a várias velocidades", disse, ainda que acredite que as organizações vão começar a abraçar o tema: "Parece que é a primeira vez que empresas em Portugal foram atacadas — não foi".

Contudo, este risco "vai acompanhar" as empresas na sua migração para o digital, admitiu Grave. "Não há como fugir".

Já o Cybersecurity and Privacy Officer da Huawei Portugal, Nuno Teodoro, sublinhou que, de facto, "existe uma tendência crescente dos riscos de cibersegurança" porque todos os relatórios assim o dizem. Quanto ao que é necessário para acelerar a mudança? Um empurrãozinho.

"Muitas vezes é necessário um empurrãozinho para fazer algo – case empurrão pode ser legal ou regulatório", adiantou Teodoro. No painel esteve também presente Pedro Latoeiro, fundador do Center for Cooperation in Cyberspace, e ainda Timóteo Menezes, o Responsável pela área de Segurança de Informação e Cibersegurança da Edisoft, que referiu que a solução passa por criar empresas "ciber-resilientes".

"Mas a resiliência tem muito que se lhe diga", acautelou. "Depende do tipo de organização, da sua maturidade, [da forma] como fazemos um equilíbrio para tentar proteger o mais importante", assinalou. E, na sua opinião, o mais importante são mesmo as pessoas. "É um trabalho em equipa com os clientes para tornar as empresas ciber-resilientes". "As empresas são alvos primordiais dessas organizações, alvo de criminosos ou de agentes estatais", disse Pedro Latoeiro, recordando que o ciberespaço é também já um dos palcos da guerra. O exemplo mais óbvio e recente é o que se vem vivo de parte a parte antes, durante e depois da invasão russa da Ucrânia.

"É óbvio que a cibersegurança está na agenda internacional, bem como empresarial", continua, "mas acho que o facto de estar na agenda mediática ainda não teve a adoção efetiva, normativa", assinalou o fundador do Center for Cooperation in Cyberspace. "O ciberespaço é, na comunidade internacional, um faroeste", concluiu. ■