BANCO DE PORTUGAL
EUROSISTEMA

Carta Circular n.º CC/2023/00000025

Assunto: Carta Circular Tratamento Prudencial Phishing

A crescente digitalização das atividades de serviços financeiros, bem como o atual contexto geopolítico e económico, potenciam um risco crescente de ameaças de cibersegurança em Portugal, suscetíveis de afetar as instituições, direta ou indiretamente, através de prestadores de serviços críticos e de infraestruturas críticas ou por intermédio dos clientes dessas instituições.

Assim, é essencial que as instituições assegurem uma gestão adequada dos riscos a que se encontram expostas, designadamente o risco associado às tecnologias de informação e comunicação, com vista a proteger a sua solvabilidade e a evitar disrupções na sua atividade, prejudicando a estabilidade do sistema financeiro.

No domínio do risco associado às tecnologias de informação e comunicação, o *phishing* – na aceção lata do termo, i.e., incluindo modalidades de *vishing*, *smishing* e outro tipo de técnicas de engenharia social, conforme termos definidos no glossário de conceitos do Centro Nacional de Cibersegurança[1] – tem vindo a assumir uma relevância crescente, dado o aumento expressivo de casos identificados nos últimos meses. Como tal, tendo presente o quadro legal e regulamentar vigente, justifica-se transmitir um conjunto de recomendações com vista a assegurar a minimização dos impactos associados a eventos de *phishing*.

Nestes termos, o Banco de Portugal, após consultar o Banco Central Europeu e o Centro Nacional de Cibersegurança, no âmbito dos poderes que lhe são atribuídos pelos artigos 14.º e 17.º da Lei n.º 5/98, de 31 de janeiro (Lei Orgânica), e ao abrigo do disposto nos artigos 92.º e 115.º-T do Regime Geral das Instituições de Crédito e das Sociedades Financeiras, aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro (RGICSF) e nos artigos 60.º, n.º 3 e 70.º, n.º 3 do Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica, aprovado pelo Decreto-Lei n.º 91/2018, de 12 de novembro (RJSPME), transmite às instituições de crédito, instituições de pagamento e instituições de moeda eletrónica com sede em Portugal, e às sucursais de instituições destes tipos, autorizadas a exercer atividade em Portugal com sede em países que não sejam Estados-Membros da União Europeia, o seguinte:

Deveres de comunicação

A ocorrência de situações de burla, de fraude, ou de natureza similar, com recurso a técnicas de *phishing,* em contas de titulares junto das instituições ("incidentes de *phishing*")[2], constitui: i) um incidente de cibersegurança, na aceção da alínea c) do n.º 2 do artigo 1.º da Instrução n.º 21/2019 do Banco de Portugal, relativa ao dever de reporte de incidentes de cibersegurança significativos; e ii) um incidente de segurança, no âmbito da Instrução n.º 1/2019 do Banco de Portugal, relativa ao reporte de incidentes de

[1] https://www.cncs.gov.pt/pt/glossario/#linhasobservacao.
[2] A presente Carta-Circular cinge-se aos eventos de *phishing* dirigidos a clientes das instituições, sem prejuízo da aplicabilidade destas e outras recomendações e requisitos na gestão dos eventos de *phishing* dirigidos a colaboradores das próprias instituições.

Enviada a:
Instituições de Crédito, Instituições de Pagamento e Instituições de Moeda Eletrónica.

caráter severo relacionados com a prestação de serviços de pagamento ao abrigo da Diretiva de Serviços de Pagamento Revista[3].

Nesse sentido, as instituições devem observar o dever de comunicação ao Banco de Portugal previsto nas referidas Instruções, sempre que observados os critérios aplicáveis de materialidade. Para a avaliação desses critérios, as instituições devem considerar a série de eventos, e não os eventos individuais, quando exista evidência de que estão relacionados. As instituições devem ainda observar sempre o disposto no n.º 11 do artigo 4.º da Instrução n.º 21/2019, bem como o disposto no n.º 8.3 e no n.º 8.5 da Instrução n.º 1/2019.

Adicionalmente, as instituições devem assegurar o cumprimento, de forma diligente, proativa e tempestiva, dos deveres de informação perante as demais autoridades competentes da ocorrência destes incidentes, nomeadamente do foro judicial, de proteção de dados ou da cibersegurança, com vista à eficaz resolução dos incidentes e para mitigação do potencial impacto sistémico, por contágio, dos incidentes.

Quadro de gestão de riscos

A ocorrência de incidentes de *phishing* constitui um indício de potenciais insuficiências no quadro de gestão do risco operacional das instituições, pelo que deve ser alvo de registo, monitorização, avaliação e atuação pelas funções de controlo interno, em particular pela função de gestão de riscos.

Neste âmbito, sublinha-se a importância de as instituições observarem o disposto nas Orientações relativas à gestão do risco associado às tecnologias de informação e comunicação e à segurança (EBA/GL/2019/04[4]) da Autoridade Bancária Europeia, em particular nos seguintes parágrafos: 31 alíneas (e) e (f) (gestão e recertificação de acessos), 31 alínea (g) (métodos de autenticação), 38 a 40 (monitorização da segurança), 59 e 60 (gestão de problemas e incidentes em matéria de tecnologias de informação e comunicação), 91 (comunicação de crises) e 92 a 98 (gestão da relação com os utilizadores de serviços de pagamentos).

Perdas operacionais

A ocorrência de incidentes de *phishing* pode originar encargos financeiros diretos relacionados com a sua resolução e pode também constituir um indício de potencial perda futura decorrente, por exemplo, da obrigação de ressarcir os clientes por instauração de processo judicial por estes junto dos órgãos competentes. Neste sentido, as instituições devem dispor de métodos adequados para o registo de perdas operacionais, incluindo sobre as estimativas para constituição de provisões consideradas necessárias, que salvaguardem o cumprimento: (i) das regras contabilísticas aplicáveis, em cumprimento do Aviso n.º 5/2015 do Banco de Portugal, nomeadamente, para este efeito, do disposto na Norma Internacional de Contabilidade relativa a Provisões, passivos contingentes e ativos contingentes; (ii) das obrigações de reporte para efeitos de supervisão, designadamente as previstas no Regulamento de Execução (UE) 2021/451 da Comissão, de 17 de dezembro de 2020; e (iii) dos requisitos em matéria de autoavaliação do capital interno, incluindo em termos reputacionais, conforme previsto no artigo 115.º-J do RGICSF e na Instrução n.º 3/2019 do Banco de Portugal.

[3] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

[4] Incorporadas no ordenamento regulamentar nacional conforme divulgado através da Carta Circular n.º CC/2020/00000029.

As instituições devem registar estes incidentes na sua base de dados de eventos de perda de risco operacional, e fundamentar devidamente a decisão sempre que entendam não registar uma perda operacional associada no caso de incidentes significativos de *phishing* dirigidos a clientes.

O Banco de Portugal continuará a intensificar as suas ações de supervisão nesta matéria, em articulação com o Banco Central Europeu no contexto do Mecanismo Único de Supervisão e em colaboração com as outras autoridades nacionais competentes relevantes, tomando em consideração os principais riscos e vulnerabilidades para a atividade das instituições de crédito, instituições de pagamento e instituições de moeda eletrónica e com particular foco nas dimensões suprarreferidas.