



## Fórum de Indústria para a Cibersegurança e Resiliência Operacional - Súmula de reunião extraordinária.

<b>Data</b>	21.02.2022
<b>Local</b>	<i>Teams Meeting</i>
<b>Participantes</b>	<b>Presenças</b>  Banco de Portugal: ADM, DPG, DSI, DSP.  Indústria: APB; BAI; Bankinter; BCP; BPI; BST; CGD; CEMG; CNCS; EuroBic; GCA; Haitong; NVB; SIBS FPS.
<b>Agenda</b>	<ol style="list-style-type: none"><li>0. Abertura</li><li>1. Introdução</li><li>2. <i>Tour-de-table</i> [(i) os impactos do incidente de cibersegurança que afetou um prestador de serviços de telecomunicações; ii) o cenário atual de cibersegurança, no contexto de outros incidentes significativos e do clima de tensões geopolíticas; iii) preocupações, ações tomadas e práticas a partilhar neste contexto.]</li><li>3. Encerramento</li></ol>



---

### **Principais conclusões:**

O CNCS informou os membros do Fórum sobre o cenário de ameaças à cibersegurança que se verifica atualmente, destacando que atualmente não existem sinais de que as instituições financeiras possam vir a ser alvos preferenciais destes atores maliciosos. O CNCS destacou que os ataques ocorridos recentemente, cerca de dois por semana, visaram na sua maioria a realização de ações destrutivas, com impactos reputacionais significativos, e através da utilização de credenciais de acesso comprometidas, obtidas através da *DarkWeb*.

Um dos membros descreveu a existência de impactos transacionais pouco significativos, decorrentes do ciberataque a um prestador de serviços de telecomunicações, tendo sido possível a reposição parcial do serviço, graças à existência de serviços redundantes no contexto do seu plano de continuidade de negócio.

Outro dos membros partilhou a sua experiência na resposta ao impacto sentido na sequência do mesmo ciberataque, na qual foi possível recuperar a maioria dos serviços impactados nas primeiras 24 horas.

O Banco de Portugal concluiu a reunião fazendo uma leitura positiva dos contributos recebidos e reforçando a importância da existência de controlos preventivos e de planos de continuidade de negócio e recuperação de desastre adequados e devidamente testados.