Cibersegurança

Dec. Lei 65)

Álvaro Magalhães

Administração de Redes II

2023

Conteúdos

Conceitos e demonstrações

Casos de notícia

Regime Jurídico de Segurança no Ciberespaço

Panorama atual

- Internet tem muitos pontos **positivos**, mas também muitos pontos **negativos**
- Uso da Internet no local de trabalho é cada vez mais uma **necessidade**
- Digitalização de processos trás **mais valias** para qualquer atividade (+simples, +rápido, +barato)
- Digitalização de **atividades ilegais** implica os mesmos benefícios para os criminosos!

Bandidos digitais

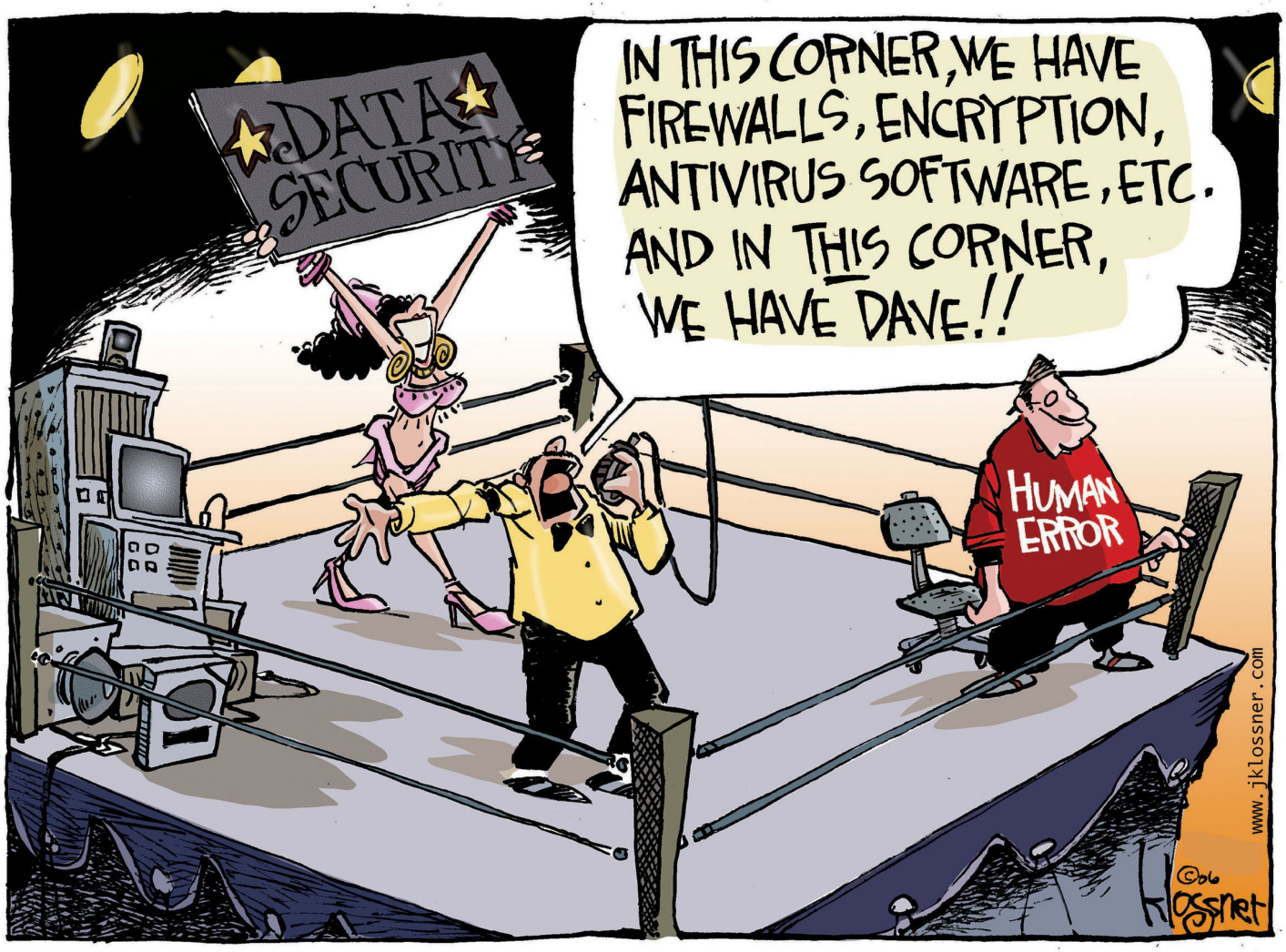
- Bandidos tentam **manipular** pessoas
- Tanto agem **sozinhos**, como em **grupos organizados**
- Desproporcionalidade **favorece** atacante
- Têm **mais competências técnicas** que os atacados
- Conseguem **gerar milhares** de ataques facilmente e sem grande custo
- Implementar soluções tecnológicas de **proteção tem custos** associados
- Organização tem de **defender 100%** dos ataques, já ao bandido basta que **um funcione**!

Em resumo

- Tecnologia é **complicada**, sempre a **evoluir**
- Novas tecnologias são **adotadas diariamente** pelas organizações
- É uma **batalha sem fim**, sem **solução mágica**
- Proteção **compete a todos**!

Nós somos o elo mais fraco...

... mas temos de ser parte da solução!



Phishing

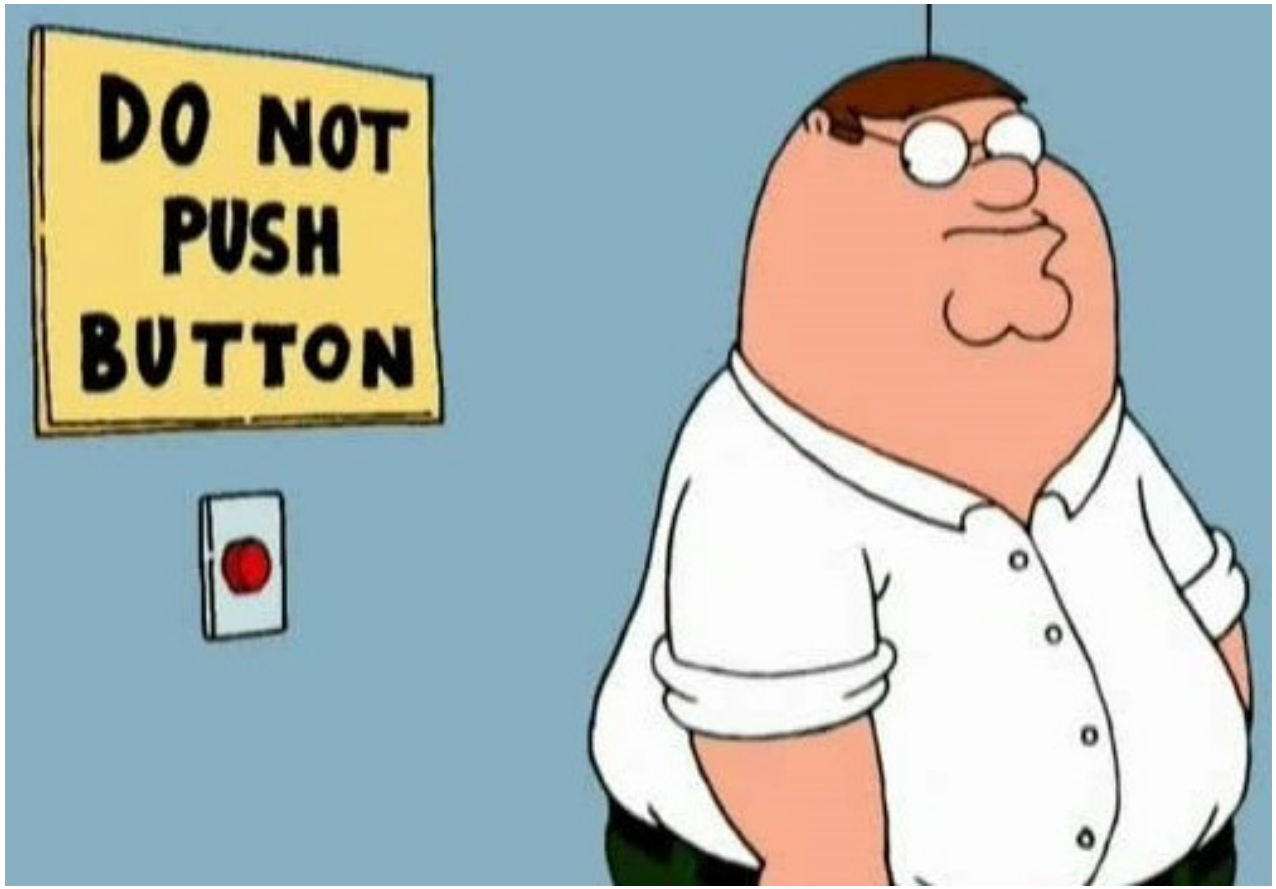
(ou pescar à rede)

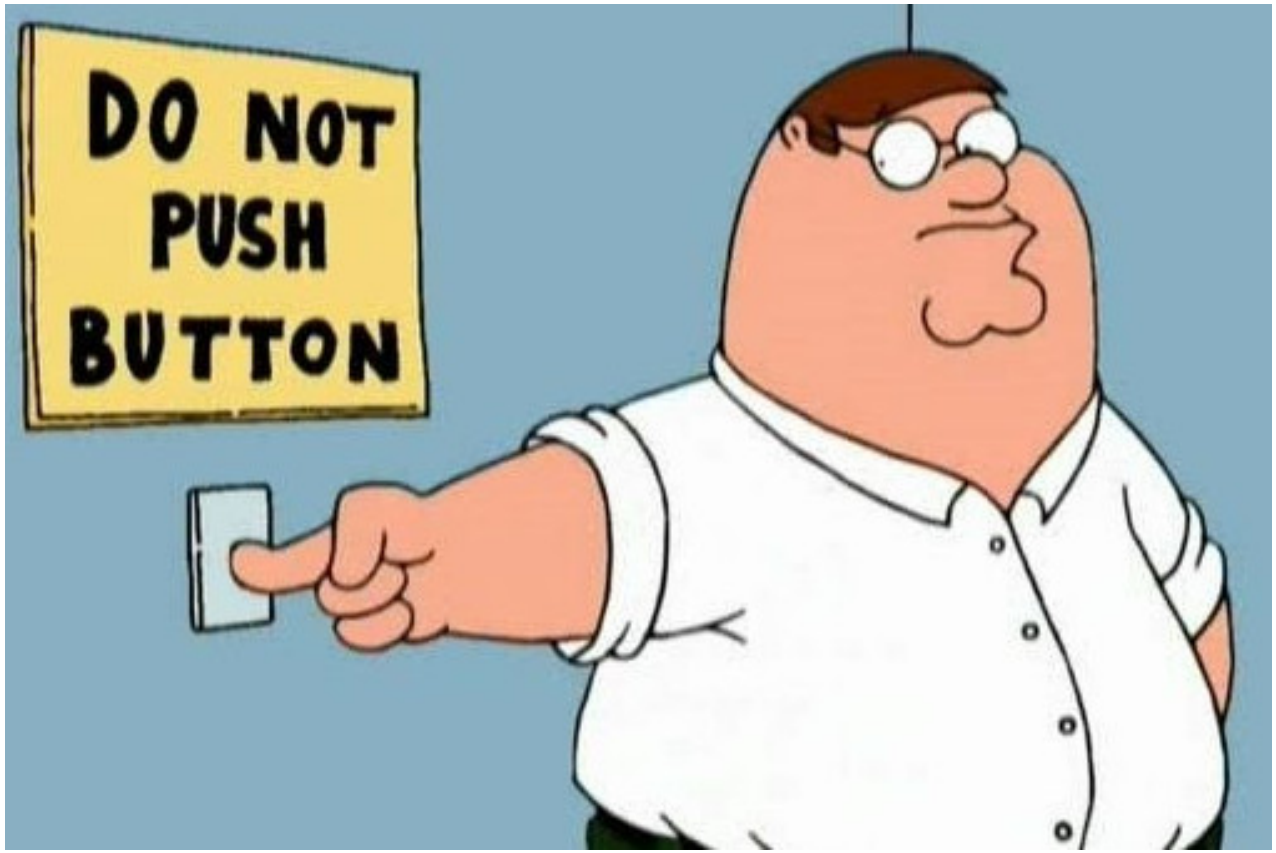
- **Ataque** de engenharia social sob a forma de **e-mail**, **SMS** ou qualquer outro tipo de mensagem eletrónica
- Querem obter **informação**, palavras **passe**, **dinheiro** disseminar *malware*, entre outros
- Também referido como **spear-phishing**, se for um ataque **dirigido**

Tentação e Urgência – Combinação muito explorada

Criar a sensação de **urgência**, para que a pessoa reaja **rapidamente**, sem pensar muito no assunto!

Ponderar, só depois agir!





Maioria dos ataques informáticos acontecem porque alguém **clicou** em algo que **não era suposto**!

Como pode um email ser perigoso?

- Inclusão de **links falsos** para levar utilizadores a abrir **páginas** de Internet **perigosas**
- Utilização de **endereços** de remetente **falsos**
- **Anexar** vírus ou documentos que contém **vírus** (imagens, docx,xlsx,pptx,zip. . .)
- Incluir **ofertas** ou anúncios com **motivações malignas** escondidas

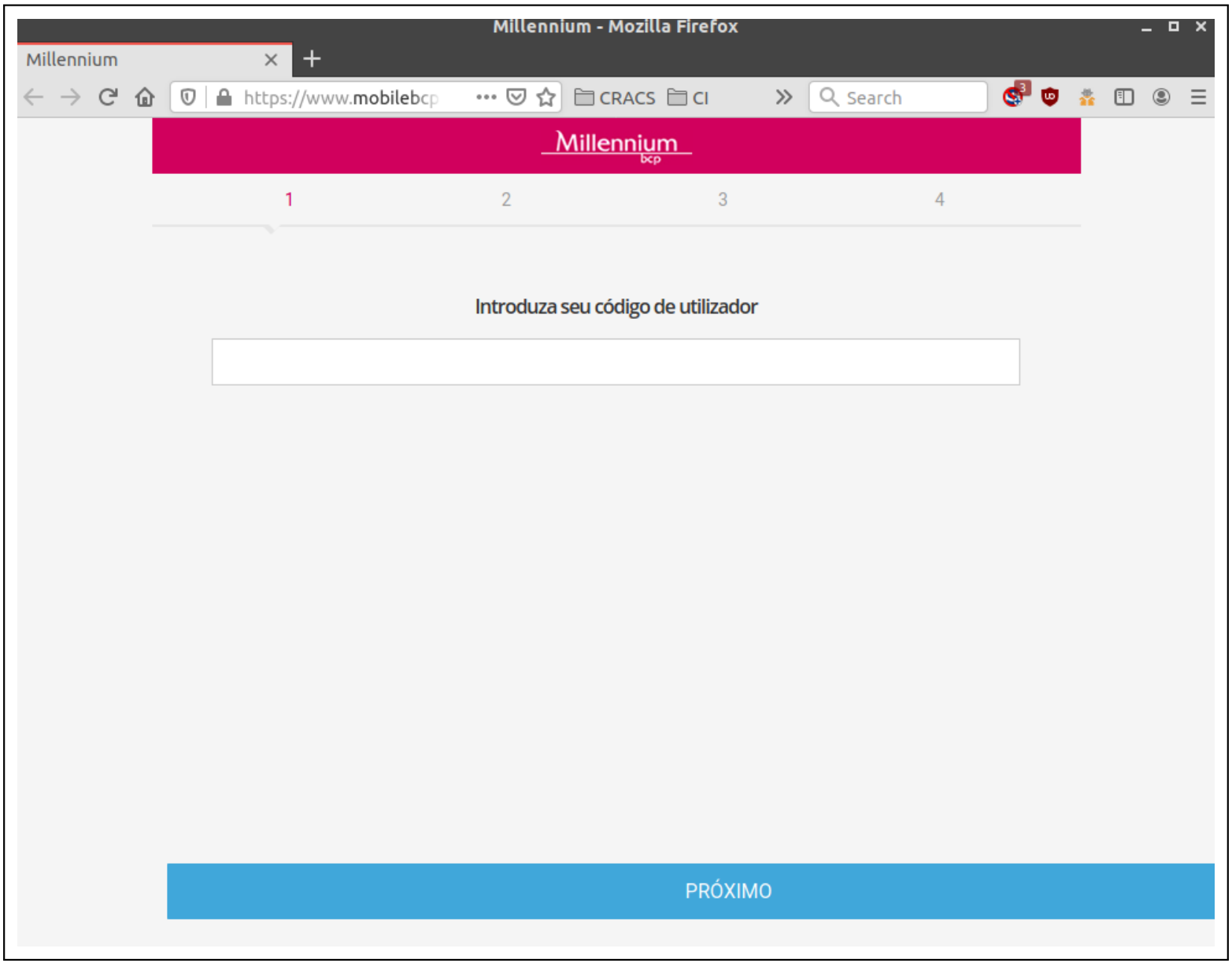
Demonstração
PHISHING

Phishing por SMS - Millennium

- **Link** abria **cópia** página de login do **banco**

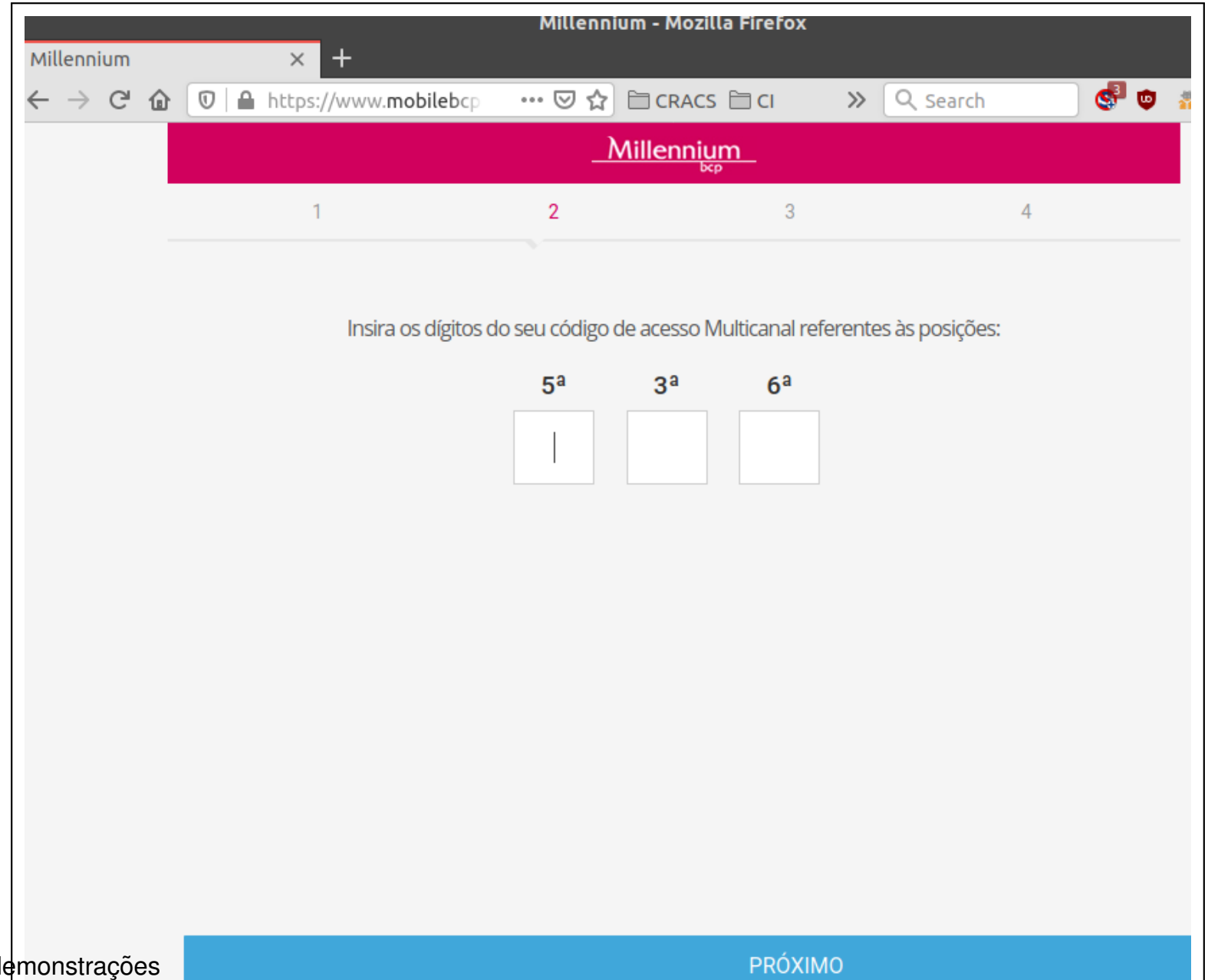
Phishing por SMS - Millennium

Passo 1 - Pedido de utilizador



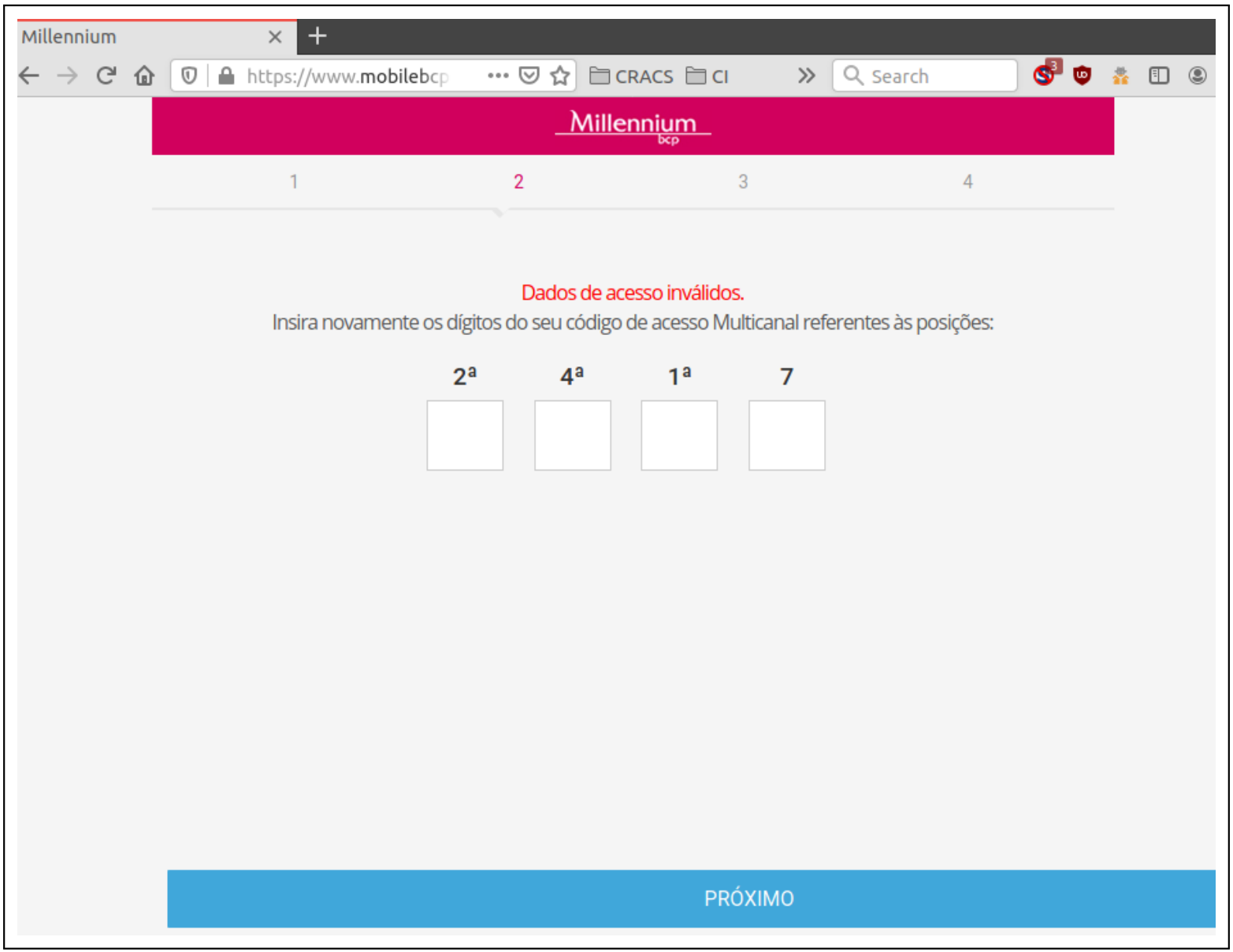
Phishing por SMS - Millennium

Passo 2 - Pedido de alguns dígitos do código



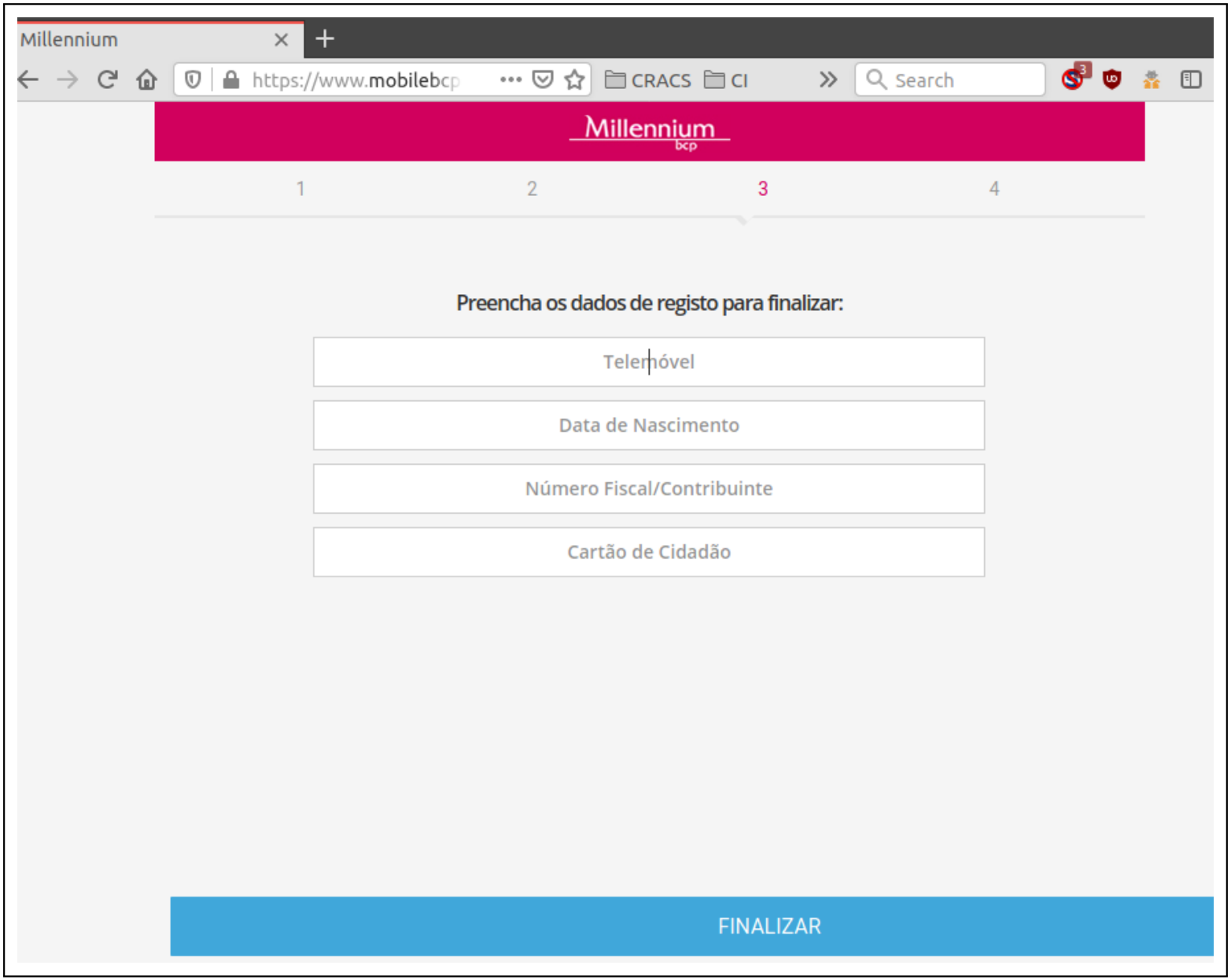
Phishing por SMS - Millennium

Passo 3 - Erro, pedindo os dígitos em falta



Phishing por SMS - Millennium

Passo 4 - Já agora, pede-se o resto...



Ransomware

(ou pedido de resgate)

- **Ataque** que encripta os **ficheiros** do computador do utilizador, tornando-os **inacessíveis**
- Atacante pede **resgate** para divulgar **chave** de desencriptação
- Ataques **indiscriminados**, de múltiplos atacantes
- Pedem pagamento em **criptomoeda**, para manter **anonimato**

Demonstração
RANSOMWARE

Dispositivos maliciosos

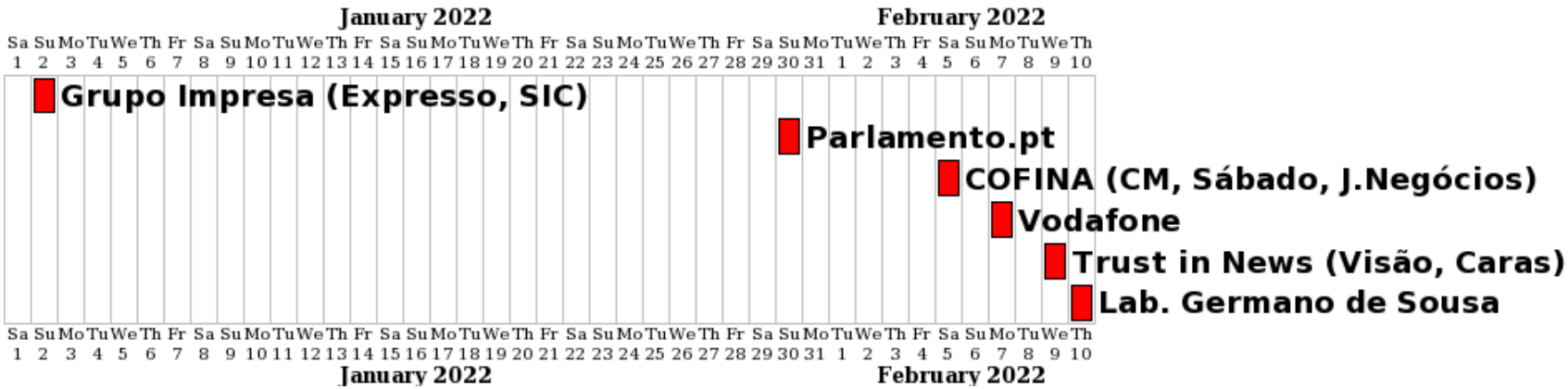
- Dispositivos **desenvolvidos** para fazer **mal**
- Podem **danificar o hardware** (*USB killer*)
- **Executar programas** ou ações definidas pelos bandidos

Demonstração
USB Malicioso

Conteúdos

Ciberataques 2022

Cronologia



Referências:

`https://www.sabado.pt/portugal/detalhe/cronologia-de-um-pais-sob-ataque-informatico-o-ultimo-foi-a-vodafone`

`https://sicnoticias.pt/pais/milhares-de-doentes-ainda-esperam-pelos-resultados-apos-o-ataque-infor`

Grupo Impresa

2 de janeiro de 2022

- Sites Expresso e SIC **em baixo durante dois dias**
- Reivindicado pelo grupo LAPSU$
- Intrusão na **rede interna**
- Controlo da plataforma de **cloud** (AWS)
- Houve **perda permanente** de dados

Site Parlamento.pt

30 de janeiro de 2022

- Site alvo de ataque (**não confirmado**)
- Reivindicado em nome do grupo LAPSU$, que mais tarde negou envolvimento
- **Serviços desligaram** temporariamente o site
- Serviços **não conseguiram** confirmar/desmentir ataque
- Impacto na **disponibilidade** do site e na **imagem da instituição**

Grupo Cofina

6 de fevereiro de 2022

- Sites do grupo indisponíveis no fim de semana (SÁBADO, Correio da Manhã, Record e Jornal de Negócios)
- Ataque não reivindicado
- Impacto na **disponibilidade** dos sites e na **imagem da instituição**

Vodafone

7 de fevereiro de 2022

- Ataque informático tornou **rede indisponível**
- **Impacto máximo** o nível dos serviços
- Afetou a **rede Multibanco, hospitais, bombeiros, acesso à televisão e rede telemóvel**
- **Uma semana para repor serviços**, ainda que não totalmente

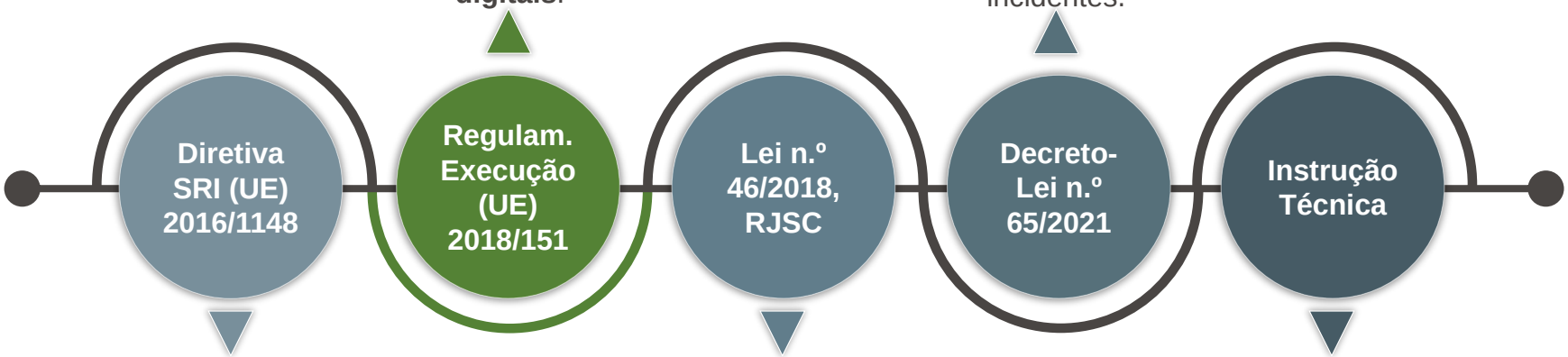
Laboratórios Germano de Sousa

10 de fevereiro de 2022

- Ataque *ransomware*
- Provavelmente via *phishing*
- **Afetou completamente** a empresa
- **Muitos milhares de doentes** não receberam resultados em tempo útil
- **Mais de duas semanas para repor serviços**

Conteúdos

Enquadramento legal



Relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Define os requisitos de segurança e as regras para a notificação de incidentes, a serem cumpridos pelos **prestadores de serviços digitais**.

Estabelece o Regime Jurídico da Segurança do Ciberespaço:

- definindo os requisitos de segurança e as regras para a notificação de incidentes; e
- identificando os **operadores de serviços essenciais**.

Regulamenta o Regime Jurídico da Segurança do Ciberespaço, definindo os requisitos de segurança e as regras para a notificação de incidentes.

Regulamento que configura uma Instrução Técnica complementar ao Decreto-Lei n.º 65/2021.

Como se aplica

Indicação de, pelo menos, um **ponto de contacto permanente** e um **responsável de segurança**.

Elaboração e atualização de um **inventário de todos** os ativos essenciais para a prestação dos respetivos serviços.

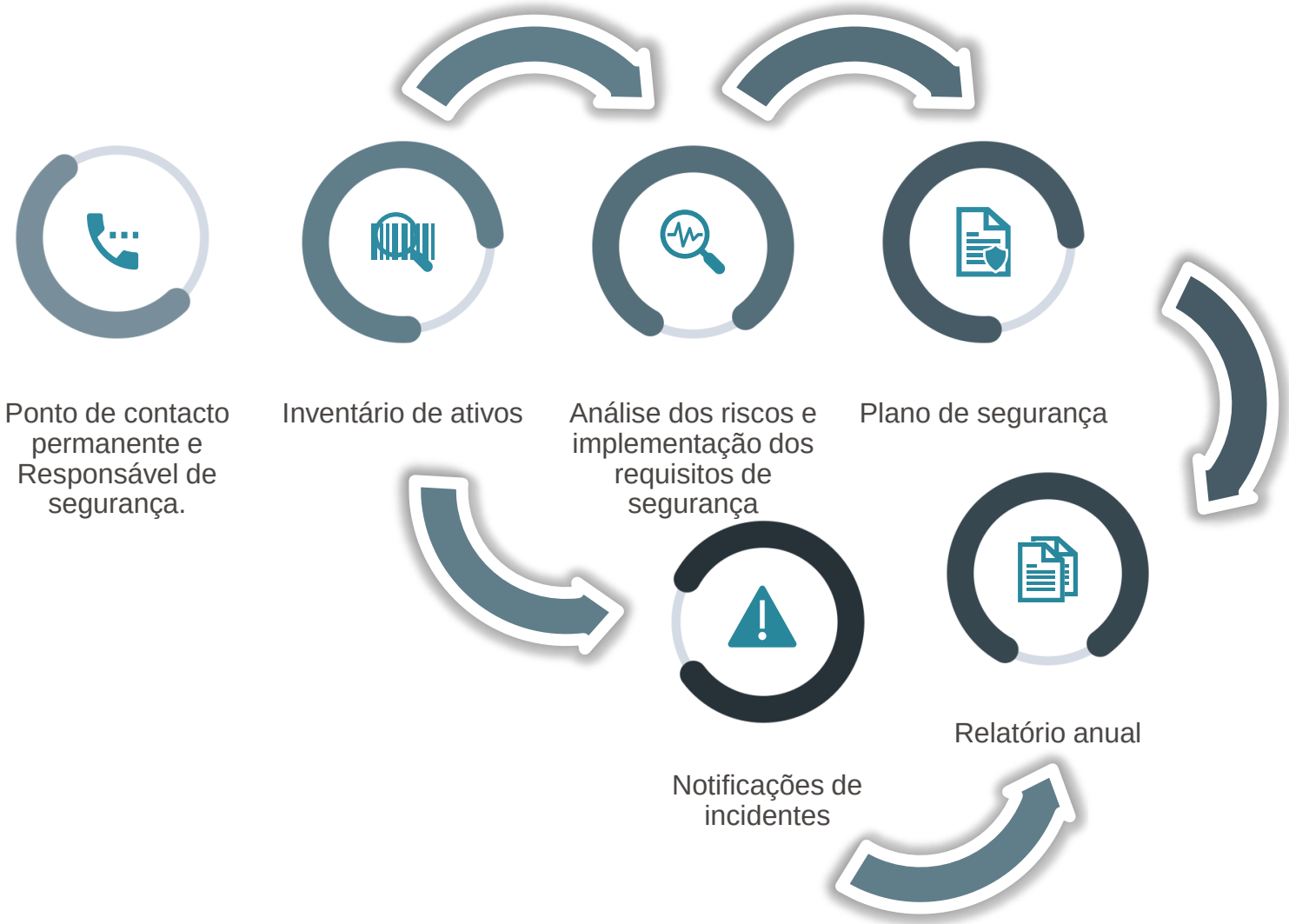
Realizar uma **análise dos riscos** em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam.

Elaboração e atualização de um **plano de segurança**, identificando medidas e organizativas para gerir os riscos identificados.

Elaboração de um **relatório anual**.

Implementar os meios e os procedimentos necessários à deteção, à avaliação do impacto e à **notificação de incidentes** com impacto relevante ou substancial.

OBRIGAÇÕES DAS ENTIDADES



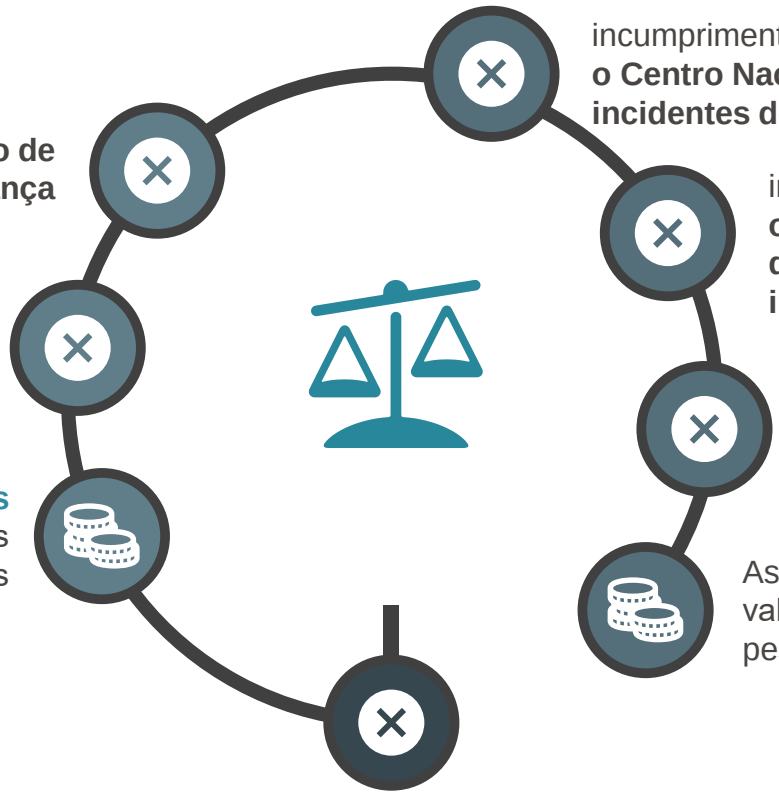
Sanções previstas

muito graves

incumprimento da **obrigação de implementar requisitos de segurança**

incumprimento de **instruções de cibersegurança emitidas pelo Centro Nacional de Cibersegurança**

As contraordenações **muito graves** podem ter valores entre os 10.000€ e os 50.000€, para pessoas coletivas



graves

incumprimento da **obrigação de notificar o Centro Nacional de Cibersegurança de incidentes de segurança da informação**

incumprimento da **obrigação de notificar o Centro Nacional de Cibersegurança do exercício de atividade no setor das infraestruturas digitais**

incumprimento da **obrigação de notificar o Centro Nacional de Cibersegurança d identificação como prestador de serviços digitais**

As contraordenações **graves** podem ter valores entre os 3.000€ e os 9.000€, para pessoas coletivas

A negligência é punível

Conclusão

Sabe a resposta?

- A sua organização já cumpre com o RJSC?
- Quanto tempo precisa para recuperar de um incidente de cibersegurança?