CNCS
Centro Nacional de Cibersegurança PORTUGAL

Observatório de Cibersegurança

RELATÓRIO EM 15 MINUTOS

CIBERSEGURANÇA EM PORTUGAL

Riscos & Conflitos

4ª EDIÇÃO

JUNHO DE 2023

PRR Plano de Recuperação e Resiliência

REPÚBLICA PORTUGUESA

Financiado pela União Europeia NextGenerationEU

“AO LONGO DE 2022, OCORRERAM DIVERSOS CIBERATAQUES DE GRANDE IMPACTO SOCIAL E NAS INFRAESTRUTURAS E SERVIÇOS EM PORTUGAL.”

CNCS
Centro Nacional de Cibersegurança
PORTUGAL

Observatório de Cibersegurança

SUMÁRIO EXECUTIVO

A segurança no ciberespaço é cada vez mais relevante na vida das pessoas, das organizações e da comunidade como um todo. Considerar o ciberespaço como uma esfera paralela não é rigoroso face à sua presença em praticamente todas as dimensões da vida económica e social. Por estas razões, o *Relatório Cibersegurança em Portugal – tema Riscos & Conflitos*, no contexto das análises às ameaças à segurança, propõe uma perspetiva centrada na segurança do ciberespaço, considerando as particularidades sociais e técnicas deste domínio.

Na sua quarta edição, este documento do Observatório de Cibersegurança do Centro Nacional de Cibersegurança (CNCS) recolhe os contributos estatísticos e qualitativos de diversas entidades no país que têm visibilidade sobre as ameaças e a sua expressão no ciberespaço de interesse nacional, quer porque são autoridades na matéria, quer porque desempenham funções de apoio à sociedade que lhes permite ter um olhar relevante. Com base nesta recolha e na produção de dados próprios do CNCS, o presente relatório faz um estudo integrado das diversas perspetivas de uma forma que se pretende coerente e abrangente, com particular incidência sobre o ano anterior, neste caso 2022, mas elaborando sobre tendências para 2023 e 2024. O objetivo é disponibilizar à comunidade uma leitura sobre as principais ameaças ao ciberespaço, de modo a fundamentar a definição de estratégias, políticas públicas e análises de risco multissetoriais.

A estrutura do documento divide-se em duas partes principais. Por um lado, a apresentação de dados sobre os incidentes de cibersegurança e os indicadores de cibercrime a afetar o ciberespaço de interesse nacional em 2022. Por outro, considerações sobre as ameaças, tendências e desafios que se colocaram nesta esfera em 2022, mas tendo em conta igualmente 2023 e 2024.

1. ANÁLISE GLOBAL

De seguida apresenta-se uma análise global que procura servir de súmula ao documento e disponibilizar uma visão integrada sobre o estado da cibersegurança no país, evitando visões fragmentadas sobre a matéria.[1]

AMEAÇAS

Os números de incidentes de cibersegurança e de cibercrimes a afetar o ciberespaço de interesse nacional continuaram a aumentar em 2022, verificando-se, em particular, um crescimento significativo de incidentes com elevado potencial disruptivo e de crimes tipificados na Lei do Cibercrime (crimes informáticos).

Os números de incidentes e de indicadores de cibercriminalidade continuaram a aumentar. Verificou-se um incremento na sofisticação e impacto de alguns incidentes, como é o caso dos que se referem a *ransomware*, e dos que afetaram organizações com elevada visibilidade social. Os crimes registados pelas autoridades policiais no âmbito específico da Lei do Cibercrime (crimes informáticos) aumentaram significativamente. Por sua vez, os registos de crimes de burla informática/comunicações diminuíram, mas tal deveu-se a alterações metodológicas.[2] Apesar destas tendências, o ritmo de crescimento no número de incidentes registados pela Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT) e de denúncias ao Gabinete Cibercrime da Procuradoria-Geral da República (PGR) diminuiu face a anos anteriores. Além disso, registaram-se menos processos de atendimento e apoio na Linha Internet Segura (LIS).

> “OS NÚMEROS DE INCIDENTES E DE INDICADORES DE CIBERCRIMINALIDADE CONTINUARAM A AUMENTAR”

1. Para uma compreensão mais aprofundada sobre a metodologia utilizada e a taxonomia desenvolvida para realizar a análise integrada dos dados apresentados, consultar a nota metodológica no final deste relatório.
2. O registo pelas autoridades policiais de burlas informáticas/comunicações, ao contrário de anos anteriores, decresceu, mas em consequência de alterações metodológicas na sua recolha: alguns crimes antes registados como “burla informática/comunicações” passaram a ser registados como “abuso de cartão de garantia ou de crédito” (não relacionado com a informática), fruto de alterações no artigo 225º do Código Penal.

As ciberameaças a afetar o ciberespaço de interesse nacional em 2022 de modo mais relevante foram o *ransomware*, a cibersabotagem/indisponibilidade,[3] o *phishing*/*smishing*/*vishing*, a burla *online*, outras formas de engenharia social e o comprometimento de contas/tentativa de *login*.

Tendo em conta a frequência e o potencial de impacto dos incidentes e cibercrimes analisados, verificou-se um aumento do número e relevância dos incidentes de *ransomware*, bem como a emergência de alguns casos de cibersabotagem/indisponibilidade de serviços digitais com impacto social, que incluíram incidentes de negação de serviços distribuída (DDoS). Em termos de frequência, os casos de *phishing, smishing* e *vishing* e a burla *online*, particularmente ligados a engenharia social (técnicas de manipulação de indivíduos), continuaram a ser muito frequentes, quer como incidentes, quer como crimes. Com elevado potencial de impacto, e por vezes ligados a casos de cibersabotagem e engenharia social, encontram-se os incidentes de comprometimento de contas e tentativa de *login*, resultantes de palavras-passe comprometidas e de exfiltrações de dados pessoais, de ataques de força-bruta ou mesmo do contorno ao duplo fator de autenticação.

Em termos de casos com elevado impacto em Portugal, durante o primeiro trimestre de 2022 ocorreu um conjunto de ações maliciosas com efeitos muito disruptivos. O ano foi marcado por ataques de *ransomware*, redundando, por vezes, em divulgação de dados.

Ao longo de 2022, ocorreram diversos ciberataques de grande impacto social e nas infraestruturas e serviços em Portugal. Poderá ter sido dos anos com o maior número de incidentes com este nível de efeito, desde que há registos, resultando numa visibilidade muito grande do tema na opinião publicada.[4]

3. Alguns casos identificados como "cibersabotagem" neste documento são categorizados como "modificação não autorizada" na taxonomia do CERT.PT. O mesmo se aplica aos casos de *ransomware*. Não obstante, considerando as taxonomias utilizadas pelos parceiros do presente documento e a necessidade de comunicar da melhor maneira possível as caraterísticas dos incidentes em causa, optou-se pelas designações apresentadas. Para uma explicação mais aprofundada desta questão, consultar a nota metodológica no final deste documento.

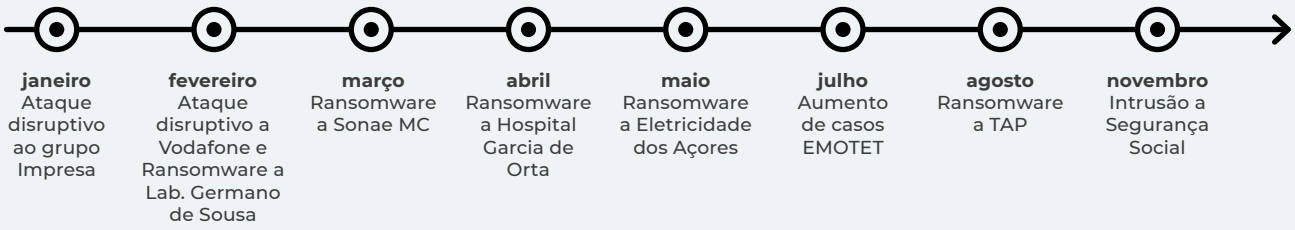
4. Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos.

O primeiro trimestre ficou marcado por quatro incidentes que, além de provocarem interrupções graves em serviços, foram percecionados pela generalidade dos cidadãos como ameaças prementes no ciberespaço. O ataque disruptivo ao grupo Impresa, afetando o setor dos *media* e o jornalismo, redundou na receção de uma mensagem pelos utilizadores de uma plataforma desta organização, enviada pelos atacantes, tendo um efeito na perceção de ameaça social. O caso que afetou a Vodafone, também com consequências sobretudo disruptivas, além de ter implicado uma grande mediatização da situação, provocou interrupções nos serviços da empresa de telecomunicações sentidas por muitos utilizadores. No mesmo mês, os utentes do Laboratório Germano de Sousa, fruto de um ataque de *ransomware*, viram os serviços desta entidade ficarem inacessíveis. Os clientes da Sonae MC, por sua vez, sentiram os efeitos do *ransomware* sofrido por esta organização na indisponibilidade do cartão de cliente.

Depois deste período particularmente impactante, é de destacar o ataque de *ransomware* ao Hospital Garcia de Orta, em abril; outro ataque de *ransomware* à Eletricidade dos Açores, em maio; o aumento de atividade ligada ao Emotet, em julho – trata-se de um *malware* que se distribui via *emails* fraudulentos e pode colocar em causa informação bancária, por exemplo; o ataque de *ransomware* à TAP, em agosto, que resultou na exposição de dados dos clientes da companhia aérea; e a intrusão em plataforma da Segurança Social, em novembro, através do comprometimento de conta, sem efeitos relevantes nos dados dos cidadãos, mas com impacto em termos de alarme social.

Figura 1

CRONOLOGIA DE ATAQUES NO CIBERESPAÇO COM IMPACTO ELEVADO EM PORTUGAL, 2022*



*Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos

Fonte: CNCS

Os agentes de ameaça a atuar no ciberespaço de interesse nacional em 2022 com mais relevância foram os cibercriminosos, os atores estatais e os hacktivistas.

Durante 2022, entre os agentes de ameaça que atuaram no ciberespaço de interesse nacional, os cibercriminosos continuaram a ter muita relevância, agindo, maioritariamente, com o propósito de obter ganhos económicos, mediante ataques de *phishing*, *smishing* e *vishing*, *ransomware* e burlas *online*, mas não só. Algumas ações destes grupos e indivíduos, embora com muito impacto, redundaram em disrupção dos alvos e benefício reputacional-mediático do atacante e não em ganhos económicos efetivos como inicialmente expectável, verificando-se um leque de fins e modos de organização difusos, tornando a sua caracterização mais ambígua, isto é, entre o cibercrime, o cibervandalismo e o hacktivismo.

Os atores estatais e paraestatais também desenvolveram atuações maliciosas no ciberespaço de interesse nacional, nomeadamente de ciberespionagem. Algumas destas ações enquadraram-se no contexto da guerra na Ucrânia e respetivos antagonismos geoestratégicos. Também fruto deste contexto, verificou-se a existência de ações de grupos hacktivistas, de cunho patriótico, que procuraram impactos mediáticos de modo a afirmarem a sua causa e ideologia, tendo em conta o alinhamento político de Portugal nesta matéria.

Constata-se que a guerra na Ucrânia teve um efeito no ciberespaço de interesse nacional principalmente ao nível da tipologia/tipo de ataques e não tanto na quantidade de incidentes. Dado o caráter geoestratégico do cenário de ameaças, diferentemente do cenário de pandemia da Covid-19, ações de recolha de informação e de cibersabotagem ganharam uma nova relevância.

Através da visualização do quadro um, acede-se a uma panorâmica relativamente ao cruzamento entre as principais ciberameaças sentidas em Portugal durante 2022 e os agentes de ameaça mais relevantes. Por exemplo, se o *ransomware* e a burla *online* são mais típicos do cibercrime, isto é, dos agentes de ameaça que procuram ganhos económicos diretos, a cibersabotagem e a ciberespionagem são mais comuns nos atores estatais, que tendem a pretender benefícios estratégicos. Os hacktivistas, tradicionalmente menos sofisticados e com pouca variedade no seu *modus operandi*, tendem para ações de disrupção, como a cibersabotagem e a indisponibilidade, acompanhadas de afirmações ideológicas no espaço mediático.

Atendendo a algumas ciberameaças em particular, o *phishing/smishing/vishing*, sendo típico do cibercrime, pode ser praticado por atores estatais, nomeadamente o *spear phishing* (*phishing* dirigido a vítimas específicas), tendo como alvo responsáveis do Estado ou de operadores de serviços essenciais. Os ataques de *ransomware* tendem a ser realizados por cibercriminosos extorsionistas, mas existem grupos deste tipo associados a alguns Estados, que são acionados a título de ação disruptiva e a coberto de falsa bandeira. A burla, por sua vez, é realizada quase sempre por criminosos comuns.

Estas ciberameaças concretizam-se frequentemente de modo articulado. Por exemplo, o *phishing* pode conduzir a um comprometimento de conta e mesmo a um ataque de *ransomware*. A engenharia social pode permitir o contorno do múltiplo fator de autenticação, uma intrusão e posterior cibersabotagem.

Quadro 1

QUADRO DE AMEAÇAS: CIBERAMEAÇAS/AGENTES DE AMEAÇA CRÍTICOS EM PORTUGAL, 2022/2023

	Cibercriminosos	Atores Estatais	Hacktivistas
Ransomware			
Phishing/Smishing/Vishing			
Burla *online*			
Comprometimento de contas/tentativa de *login*			
Engenharia social (várias)			
Cibersabotagem/indisponibilidade			
Distribuição de *malware*/sistema infetado (sem considerar *ransomware*)			
Ciberespionagem			
Vulnerabilidades e sua exploração			

Agentes de ameaça e ciberameaças com relevância elevada em Portugal durante 2022/2023.
Agentes de ameaça e ciberameaças com relevância média em Portugal durante 2022/2023.
Ciberameaça com frequência elevada como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência média como prática dos agentes de ameaça em causa em Portugal.
Ciberameaça com frequência baixa ou inexistente como prática dos agentes de ameaça em causa em Portugal.

Fonte: CNCS

As vítimas de incidentes de cibersegurança mais relevantes em Portugal durante 2022 foram os setores da Banca (sobretudo clientes), da Educação e Ciência, Tecnologia e Ensino Superior, dos Transportes, da Saúde, bem como da Comunicação Social. No âmbito dos subsetores da Administração Pública, destaca-se, comparativamente, a Administração Pública Local como alvo com maior número de incidências. Por sua vez, alguns organismos públicos em particular sofreram ciberataques com significado.

Os setores mais afetados por incidentes de cibersegurança em Portugal durante 2022 foram a Banca (sobretudo *phishing* aos clientes), a Educação e Ciência, Tecnologia e Ensino Superior, os Transportes e a Saúde. A Administração Pública em geral, mas com particular incidência na Local, também foi um alvo frequente. Certos organismos públicos foram vítimas de ciberataques que se revestiram de significado. Por fim, dado o elevado número de incidentes identificados no âmbito dos Prestadores de Serviços de Internet e Infraestruturas Digitais, indicia-se que os clientes das empresas de telecomunicações são também alvos muito frequentes, o que inclui os cidadãos em geral e as pequenas e médias empresas (PME). Com menor frequência, mas com impacto social relevante, é importante ainda considerar o setor da Comunicação Social como uma vítima em 2022. Todavia, tendo em conta dados do Eurostat referentes a 2021, as empresas portuguesas sofrem menos consequências negativas de incidentes de segurança nas Tecnologias de Informação e Comunicação (TIC) do que as suas congéneres da União Europeia (UE).

UM OLHAR SOBRE 2023 ATRAVÉS DO CERT.PT

Durante o primeiro trimestre de 2023, o número de incidentes de cibersegurança registados pelo CERT.PT decresceu 38% face ao período homólogo, passando de 754 registos em 2022 para 470 em 2023. Contudo, este valor representa uma subida de 28% relativamente ao último trimestre de 2022, no qual se registaram 366 incidentes.

A perceção de risco de alguma entidade no ciberespaço de interesse nacional poder sofrer um incidente de cibersegurança aumentou em 2022 e 2023.

Verifica-se, em 2022 e 2023, uma perceção elevada de que há um maior risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional. Esta perceção é influenciada pela guerra na Ucrânia e pelo contexto geopolítico correspondente. A influência da pandemia da Covid-19 nessa perceção ainda se fez sentir. Acresce que a perceção de que o ciberespaço de interesse nacional está mais resiliente a ciberataques decresceu.

Foram identificadas como principais tendências internacionais em termos de ameaças ao ciberespaço no presente e futuro próximo o incremento do hacktivismo e o crescimento de casos de DDoS, de exploração de vulnerabilidades e de ameaças a sistemas de controlo industrial.

Foram identificadas como tendências internacionais a influenciar os tempos vindouros o incremento do hacktivismo associado a conflitos e movimentos de protesto em relação a temas da atualidade; o aumento dos casos de incidentes de DDoS e de exploração de vulnerabilidades ainda não reveladas publicamente (*zero-day*); e ameaças a sistemas de controlo industrial.

As principais tendências nacionais, no que se refere ao quadro de ameaças no ciberespaço, são a crescente "profissionalização" do cibercrime, a incerteza resultante da guerra na Ucrânia e algumas ciberameaças específicas, tais como o *ransomware*, o DDoS, o *malware* de furto de credenciais e os *smishing/vishing/spoofing* oportunistas relativamente ao uso massificado do telemóvel.

Em termos nacionais, identificam-se como principais tendências para o presente e futuro próximo a "profissionalização" crescente do cibercrime e a persistência de ameaças de efeitos incertos resultantes da guerra na Ucrânia, como sejam as que podem advir de grupos de hacktivistas em defesa de um dos polos do conflito; o aumento dos casos de *ransomware* e outras formas de extorsão; ataques de DDoS para fins políticos ou extorsionistas; a distribuição de *malware* de furto de credenciais; a continuação de casos ligados ao uso de telemóvel (*smishing/vishing/spoofing*); a emergência de ameaças que comprometem os protocolos de pagamentos *contactless*; a persistência de

tentativas de intrusão através do comprometimento de contas; e a utilização da Inteligência Artificial (IA) como instrumento de acesso facilitado às práticas de crime no ciberespaço.

Os principais desafios ao ciberespaço de interesse nacional em 2023 e 2024 prendem-se com o aumento da superfície de ataque, a sofisticação de alguns agentes de ameaça, a dificuldade em imputar responsabilidades e a falta de literacia e de especialistas em cibersegurança.

Para 2023 e 2024 colocam-se como principais desafios à segurança do ciberespaço de interesse nacional a necessidade de mitigar a insegurança num ciberespaço mais disseminado, e por vezes fragmentado, com maior superfície de ataque, fruto da Internet das Coisas, das tecnologias móveis, das plataformas em nuvem e da tecnologia 5G (neste contexto, acrescem alguns desafios de ordem técnica e no quadro de ameaças, como o uso de IA em ciberataques ou a exploração de vulnerabilidades técnicas); a sofisticação crescente dos agentes de ameaça; a dificuldade em estabelecer mecanismos de imputação a agentes de ameaça externos; e o problema da ainda insuficiente literacia digital nos âmbitos da ciber-higiene e do conhecimento da cibersegurança como área de saber, bem como a falta de qualificação de profissionais.

CENÁRIOS DE AMEAÇAS AO CIBERESPAÇO DE INTERESSE NACIONAL

Compreender uma ameaça permite antecipar potenciais incidentes ou cibercrimes e preveni-los de modo mais eficaz. Num exercício iniciado na edição anterior deste relatório, apresenta-se no quadro dois uma panorâmica sobre os cenários de ameaças com potencial de afetar o ciberespaço de interesse nacional no presente e no futuro próximo, tendo em conta as suas características e as tendências quanto ao seu enraizamento.

O cenário de ameaças típico do contexto pandémico, muito ligado ao cibercrime e a ataques oportunistas relativamente ao trabalho remoto, ao isolamento social e a uma maior necessidade do uso do digital, apresenta-se em trajetória decrescente. Contudo, este cenário pode ainda fazer-se sentir devido a algumas práticas que permanecem, quer nos agentes de ameaça, que podem ter adquirido novos *modus operandi* que persistem, quer nos utilizadores, como seja a manutenção de algum trabalho remoto.

Como cenário persistente, mantêm-se as ameaças típicas do contexto geopolítico e estratégico atual, devido ao prolongamento da guerra na Ucrânia, o que provoca o acentuar de antagonismos que encontram formas de polarização em ações de atores estatais e hacktivistas que pretendem ganhos informacionais ou propagandísticos para o seu lado do conflito. Enquanto a guerra na Ucrânia não terminar, prevê-se que este cenário se mantenha e possa mesmo agudizar-se.

Ainda numa fase emergente, e com resultado incerto quanto à transformação que efetivamente poderá trazer, devem considerar-se as ameaças que têm vindo a surgir em resultado da disponibilização de plataformas de IA para o público em geral e o seu potencial de utilização para o desenvolvimento de ferramentas úteis na realização de ações maliciosas no ciberespaço. Esta disponibilização tem-se mostrado apta a apresentar soluções técnicas para a efetividade de ciberataques, mas também para a criação de campanhas de desinformação baseadas em imagens e textos fraudulentos. Esta massificação do cibercrime pode ser acompanhada pela utilização de formas avançadas destas tecnologias por agentes de ameaça mais sofisticados.

Em paralelo a estes cenários de diferentes intensidades, mas convivendo entre si, e por vezes reforçando-se, persiste um cenário caracterizado pelas atividades tradicionais ligadas ao cibercrime nacional e internacional e às interações sociais de utilizadores comuns que podem redundar em incidentes de cibersegurança ou em cibercrimes.

Quadro 2

CENÁRIOS DE AMEAÇAS A AFETAR O CIBERESPAÇO DE INTERESSE NACIONAL

Cenário decrescente (1) - Ameaças típicas do contexto pandémico	Cenário persistente (2) - Ameaças típicas do contexto geopolítico e estratégico da guerra na Ucrânia	Cenário emergente (3) - Ameaças típicas do contexto de facilitação do cibercrime por via da IA
Agentes de ameaça próprios deste cenário: cibercriminosos com objetivos económicos.	Agentes de ameaça próprios deste cenário: atores estatais e paraestatais com objetivos geopolíticos e estratégicos (e ameaças persistentes avançadas); hacktivistas com objetivos ideológicos.	Agentes de ameaça próprios deste cenário: *script kiddies* com objetivos reputacionais e económicos; hacktivistas com objetivos ideológicos; e cibercriminosos com objetivos económicos.
Tipologias de ações hostis emergentes neste cenário*: • burlas *online*; • comprometimento de sistemas próprios do trabalho remoto; • desinformação sobre saúde; • *phishing* massificado; • *ransomware*.	Tipologias de ações hostis emergentes neste cenário: • ciberespionagem; • comprometimento de cadeias de fornecimento; • comprometimento de contas; • comprometimento de sistemas próprios do trabalho remoto; • DDoS; • *defacements*; • desinformação sobre o conflito na Ucrânia; • exploração de vulnerabilidades; • intrusões; • *phishing* e *spear phishing*; • *ransomware* e/ou cibersabotagem.	Tipologias de ações hostis emergentes neste cenário: • abuso de IA; • burlas *online*; • comprometimento de contas; • *deep fakes*; • desinformação variada; • engenharia social; • exploração de vulnerabilidades; • *phishing*.
Temas e alvos: Banca, Saúde, serviços de *streaming*, serviços postais e de transporte.	Temas e alvos: operadores de serviços essenciais, Administração Pública e Órgãos de Soberania.	Temas e alvos: cidadão em geral, Administração Pública e Órgãos de Soberania.

Cenário 0 - Contexto permanente: a materialização dos cenários 1, 2 e 3 não obsta a que exista uma dinâmica permanente própria das ameaças ao ciberespaço de interesse nacional para lá da pandemia, do contexto internacional e da emergência da IA, âmbito no qual certos incidente e cibercrimes tendem a ocorrer.

Fonte: CNCS

*Nem todas as ações hostis consideradas relevantes são consequência sempre e necessariamente dos agentes de ameaça típicos do cenário em causa, embora tendencialmente sim.

ESTRATÉGIA NACIONAL DE SEGURANÇA DO CIBERESPAÇO 2019-2023

Os relatórios dedicados às componentes Sociedade e Riscos e Conflitos, do Observatório de Cibersegurança, têm apresentado os indicadores ligados à cibersegurança estabelecendo, sempre que pertinente, uma articulação destes com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENSC), de modo a acompanhar a concretização dos objetivos definidos por este instrumento de políticas públicas.

No que diz respeito ao tema Riscos e Conflitos, mais do que a quantidade de incidentes ou cibercrimes, as características cada vez mais complexas do quadro de ameaças ao ciberespaço de interesse nacional colocam desafios importantes à capacidade de proteção e reação aos incidentes e ao cibercrime. Por isso, a este respeito, a situação convoca em particular os eixos "2 - Prevenção, educação e sensibilização", "3 - Proteção do ciberespaço e das infraestruturas" e "4 - Resposta às ameaças e combate ao cibercrime" da ENSC. No entanto, a existência do presente documento, bem como a coordenação entre entidades que ele demonstra existir, são indicadores positivos de desenvolvimentos importantes no que diz respeito à compreensão do quadro de ameaças e à partilha de informação entre atores-chave da comunidade, um dos objetivos da ENSC e daqueles três eixos, mas sobretudo do eixo "6 - Cooperação nacional e internacional".

2. DESTAQUES

INCIDENTES E CIBERCRIME EM PORTUGAL

O número de incidentes registados pelo CERT.PT aumentou 14%, de 1781 em 2021 para 2023 em 2022 (CERT.PT).

Cerca de dois terços dos incidentes registados pelo CERT.PT ocorreram em entidades privadas e um terço em entidades públicas, em 2022 (CERT.PT).

Os setores e áreas governativas com mais incidentes registados pelo CERT.PT em 2022 foram a Banca (sobretudo clientes) (19% do total), as Infraestruturas Digitais (7%) e a Educação e Ciência, Tecnologia e Ensino Superior (7%) (CERT.PT).

O *phishing/smishing* (37% do total), a engenharia social (14%) e a distribuição de *malware* (11%) continuam a ser os tipos de incidentes com mais registos realizados pelo CERT.PT em 2022 (CERT.PT).

As marcas da Banca (59% do total), dos Transportes e Logística (17%) e dos Serviços de Email e outros (17%) são as mais simuladas nos ataques de *phishing* e *smishing* registados pelo CERT.PT em 2022, tal como aconteceu em 2021 (CERT.PT).

No âmbito do tipo de incidente de engenharia social, os subtipos mais registados pelo CERT.PT em 2022 foram o *vishing* (64% do total), a CEO Fraud (13%) e a *sextortion* (10%) (CERT.PT).

O número de incidentes de *ransomware* registados pelo CERT.PT em 2022 aumentou para quase o dobro face ao ano anterior, de 35 para 69 (CERT.PT).

O número de observáveis registados pelo CERT.PT em 2022 aumentou 43% em relação a 2021 (CERT.PT).

O tipo de observável mais registado pelo CERT.PT, em 2022, continua a ser o serviço vulnerável (91% dos casos), seguindo-se o *malware* (6%), o *botnet drone* (1%) e o *blocklist* (1%) (CERT.PT).

Os setores e áreas governativas com mais observáveis registados pelo CERT.PT foram os Prestadores de Serviços de Internet (81% dos casos), as Infraestruturas Digitais (8%) e a Educação e Ciência, Tecnologia e Ensino Superior (5%) (CERT.PT).

O tipo de incidente mais registado pelos membros da RNCSIRT foi a tentativa de *login* (14% do total), seguida do sistema infetado (*malware*) (13%) e do *phishing/smishing* (11%) (RNCSIRT).

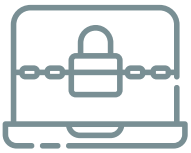
Em 2022, a CNPD registou 376 violações de dados pessoais, mais 15% do que no ano anterior (CNPD).

Cerca de 80% das entidades que notificaram violações de dados pessoais à CNPD em 2022 eram privadas. As restantes 20% eram públicas (CNPD).

Os setores e atividades privados com mais notificações à CNPD em 2022 foram o Comércio e Serviços (28% dos casos), a Banca e Seguros (15%) e a Saúde (11%). Na esfera pública, a Administração Pública Local (28%) é o subsetor do Estado com mais notificações (CNPD).

O princípio da informação mais comprometido nos casos notificados à CNPD é a confidencialidade (58% do total), seguido da disponibilidade (22%) e da integridade (20%) (CNPD).

O *ransomware* é a origem mais frequente para os incidentes de violações de dados notificados à CNPD (30% do total), seguido da falha humana (22%) e das falhas aplicacionais (13%). O *ransomware* subiu 57% face ao ano anterior (CNPD).



Segundo o IUTIC às empresas, do Eurostat e do INE, em Portugal, 11,5% das empresas com mais do que 10 empregados (excluindo setor financeiro) admitem ter sofrido consequências negativas de incidentes de segurança nas TIC em 2021. A média da UE é de 22,2%. (Eurostat).

No mesmo inquérito, o tipo de consequência de incidentes de segurança nas TIC mais frequente é a indisponibilidade de serviços TIC (9,7% em Portugal e 20,1% na média da UE) (Eurostat).

Há mais empresas grandes (20,2%) do que pequenas (10,4%) a admitirem ter sofrido qualquer consequência de incidente de segurança nas TIC, em Portugal (Eurostat).

Os crimes informáticos (Lei do Cibercrime) registados pelas autoridades policiais aumentaram 48% em 2022. Por sua vez, a burla informática/comunicações (não registada entre os crimes informáticos, mas relacionada com a informática) decresceu 2%, mas tal deveu-se sobretudo a alterações metodológicas, caso contrário, teria crescido[5] (DGPJ).

A burla informática/comunicações é o crime relacionado com a informática mais registado pelas autoridades policiais em 2022, com 20 901 registos. O crime estritamente informático (Lei do Cibercrime) mais registado foi o acesso/interceção ilegítimos, com 1012 registos, mais 60% do que no ano anterior (DGPJ).

Verificou-se um crescimento de 1% dos crimes relacionados com a informática registados pelas autoridades policiais em 2022 (crimes da Lei do Cibercrime somados a burla informática/comunicações e a devassa por meio de informática, mas com quebra de série devido a alteração metodológica no registo da burla informática/comunicações[6]). Ao mesmo tempo, verificou-se um crescimento de 14% no total de todos os tipos de crimes registados pelas autoridades (DGPJ).

A proporção de crimes relacionados com a informática no universo de todos os crimes registados pelas autoridades policiais diminuiu de 7,8% em 2021 para 6,9% em 2022 (com quebra de série devido a alteração metodológica no registo da burla informática/comunicações). Esta é a segunda vez que, desde 2009, se assiste a um decrescimento deste valor, sendo que a primeira foi em 2017 e de apenas 0,1 pp[7] (DGPJ).

O ano de 2021 foi o ano com mais condenados por crimes relacionados com informática desde 2009, com 256 condenados, um crescimento de 78% face a 2020 (DGPJ).

5. Sem a alteração metodológica, estima-se que o crescimento no número de crimes de burla informática/comunicações poderia ser na ordem dos 21%.
6. Sem a alteração metodológica, estima-se que o crescimento do total de crimes relacionados com a informática poderia ser na ordem dos 23%.
7. Sem a alteração metodológica, estima-se que a proporção de crimes relacionados com a informática no universo de todos os crimes registados pelas autoridades policiais poderia ser na ordem dos 8,4%.

O crime de burla informática/comunicações é o crime relacionado com a informática com mais condenados em 2021, com 198 casos, mais 83% do que no ano anterior, a que se segue o crime de falsidade informática com 31 condenados (DGPJ).

Entre os condenados por crimes relacionados com a informática em 2021, predominam os indivíduos do sexo masculino (65%) e com idades entre os 21 e os 29 anos (33%). A burla informática/comunicações é o crime relacionado com a informática mais praticado em todas as idades, exceto no grupo etário entre os 16 e os 17 anos, no qual o crime mais praticado é a sabotagem informática (DGPJ).

A UNC3T da PJ abriu mais 6,7% de inquéritos em 2022 do que em 2021 (PJ).

Os crimes com mais impacto entre os inquéritos abertos pela UNC3T da PJ em 2022 foram o branqueamento de capitais, a *sextortion* e o *ransomware* (PJ).

Em 2022, o Gabinete Cibercrime da PGR registou 2125 denúncias, mais 83% do que no ano anterior (PGR).

O *phishing* e diversos tipos de burlas *online* são os tipos de criminalidade mais denunciados ao Gabinete Cibercrime da PGR em 2022 (PGR).

A Linha Internet Segura registou menos 24% de processos de atendimento e apoio em 2022 do que em 2021, tendo passado de 1626 para 1236 (APAV).

Os crimes e outras formas de violência mais registados pela Linha Internet Segura em 2022 foram a burla, a *sextortion* e o furto de identidade. Relativamente ao ano anterior, a burla cresceu 85% e a *sextortion* decresceu 28% (APAV).

O número de imagens categorizadas como conteúdo sexual de menores pela Linha Internet Segura diminuiu de 1929 em 2021 para 878 em 2022, portanto, menos 54% (APAV).

AMEAÇAS, TENDÊNCIAS E DESAFIOS EM PORTUGAL

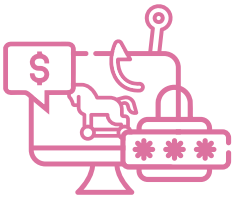
Para a quase totalidade dos profissionais inquiridos em inquérito à comunidade de entidades com colaboração com o CNCS, o risco de uma entidade sofrer um incidente no ciberespaço de interesse nacional aumentou em 2022 (para 93% dos inquiridos) e em 2023 (92%) (CNCS).

Para a grande maioria dos inquiridos do mesmo inquérito (85%), a perceção de que o risco de sofrer um incidente de cibersegurança no ciberespaço de interesse nacional aumentou é influenciada pela guerra na Ucrânia (CNCS).

Para 44% dos inquiridos, o ciberespaço de interesse nacional tem o mesmo nível de resiliência a ciberataques em 2023 do que tinha 2022. Para 41% está mais resiliente e para 14% está menos (CNCS).

Os agentes de ameaça mais relevantes a atuar no ciberespaço de interesse nacional, em 2022, foram os cibercriminosos, os atores estatais e os hacktivistas.

Os cibercriminosos realizaram principalmente ataques de *phishing*/*smishing*/*vishing*, *ransomware*, intrusões (algumas na forma tentada), diversos tipos de burla e branqueamento de capitais; os atores estatais, operações de ciberespionagem e de intrusão; e os hacktivistas, ataques com efeitos disruptivos.



As vítimas mais relevantes destes agentes de ameaça foram os setores da Banca (sobretudo clientes), da Educação e Ciência, Tecnologia e Ensino Superior, dos Transportes, da Saúde, das Telecomunicações e da Comunicação Social. A Administração Pública foi também um alvo importante.

Principais tendências internacionais para presente e futuro próximo: hacktivismo no âmbito de conflitos ou movimentos de protesto; aumentos nos volumes de tráfego direcionados para ataques DDoS; continuação de esforços para explorar vulnerabilidades "*zero-day*"; e ameaças a sistemas de controlo industrial.

Principais tendências nacionais para presente e futuro próximo: incremento da ameaça resultante da "profissionalização" crescente do cibercrime e das repercussões da guerra na Ucrânia; relevância de ameaças como o *ransomware* e outros tipos de extorsões, DDoS, *malware* de furto de credenciais, *smishing*/*vishing*/*spoofing*, ataques baseados em protocolos de pagamentos *contactless* e variados tipos de intrusões (ou tentativas); e utilização da IA como instrumento de acesso facilitado à cibercriminalidade.

Principais desafios estratégicos ao ciberespaço de interesse nacional: a cibersegurança nas tecnologias IoT, móveis, em nuvem e 5G; o incremento do recurso ao ciberespaço por parte de agentes de ameaça sofisticados; a dificuldade de responsabilização e punição de agentes de ameaça externos; e a falta de literacia digital e de recursos humanos especializados em cibersegurança.

Observatório
de **Cibersegurança**

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

Centro Nacional de Cibersegurança
Rua da Junqueira, 69 | 1300-342 Lisboa
cncs@cncs.gov.pt • (+351) 210 497 400