

bilingual edition

ptsoc {news}

NIS 2 com regras mais rigorosas

3 perguntas a **Marta Moreira Dias**

Ransomware **por Carlos Cabreiro**

08

NIS 2 with tougher rules

3 questions to **Marta Moreira Dias**

Ransomware **by Carlos Cabreiro**

•pt



03 NIS 2 com regras mais rigorosas NIS 2 with tougher rules

14 Estatísticas Statistics

Denúncias de cibercrimes continuam a aumentar. Reports of cybercrime continue to rise

Mais ataques a dados de menos pessoas. More attacks on fewer data holders.

Gestores mais conscientes das ciberameaças? Managers more aware of cyberthreats?

16 3 perguntas a... 3 questions to...

Marta Moreira Dias

Board of Directors .PT

27 Ransomware, “um crime informático puro”. Ransomware, ‘a pure computer crime’.

Carlos Cabreiro

Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), Polícia Judiciária Director of the National Unit to Combat Cybercrime and Technological Crime (UNC3T), Portuguese Criminal Police

32 Documentos Documents

Diários sobre o ransomware LockBit. LockBit ransomware diaries

Estado global da legislação sobre o cibercrime. Global state of cybercrime legislation

Como a guerra na Ucrânia alterou a paisagem das ciberameaças. How the Ukraine conflict transformed the cyberthreat landscape

Weapons of Control, Shields of Impunity: Internet shutdowns in 2022

NIS 2 com regras mais rigorosas

A [diretiva EU 2022/2055](#) (NIS 2) foi aprovada pela União Europeia (UE) e publicada no Jornal Oficial da UE a 27 de dezembro. A sua transposição para o direito nacional até 17 de outubro de 2024 “deve acompanhar dois instrumentos comunitários com ela especialmente intrincados”: a [diretiva relativa à resiliência das entidades críticas](#) (CER) e o [Regulamento \(UE\) 2022/2554](#) (DORA), relativo à resiliência operacional digital do setor financeiro, “circunstância que deverá ser acautelada também a nível nacional”, nota Marta Moreira Dias, do Board of Directors do .PT.

O grande objetivo é aumentar o nível de [cibersegurança no espaço europeu](#), mas, antecipa esta responsável, a adequação à NIS 2 “tem custos e vai ter um impacto sério nos orçamentos das entidades abrangidas. O quadro contraordenacional previsto e o nível e impacto da responsabilidade dos órgãos de gestão, provavelmente vai conduzir à procura de seguros de responsabilidade civil na área da cibersegurança”.

A anterior diretiva sobre segurança das redes e da informação ([SRI ou NIS](#), de Network and Information Security) surgiu em 2016 e tinha de ser transposta até Maio de 2018. Procurava ter medidas para “garantir um elevado nível comum de segurança das redes e da informação

NIS 2 with tougher rules

[Directive EU 2022/2055](#) (NIS 2) was approved by the European Union (EU) and published in the Official Journal of the European Union on 27 December. Its transposition into national law until 17 October 2024 ‘must accompany two community instruments especially intricate with it’: [directive on the resilience of critical entities](#) (CER) and [Regulation \(EU\) 2022/2554](#) (DORA) on digital operational resilience for the financial sector, ‘a circumstance that should also be safeguarded at national level’, notes Marta Moreira Dias, Board Member of .PT.

The main goal is to increase the level of [cybersecurity within the European space](#). However, as Moreira Dias anticipates, the adequacy to the NIS 2 ‘has costs and will have a serious impact on the budgets of the entities covered. The anticipated framework of administrative offences and the level and impact of the responsibility of management bodies will probably lead to a demand for civil liability insurances in the area of cybersecurity’.

The previous directive on security of network and information systems ([SRI or NIS](#)) came into being in 2016 and had to be transposed by May 2018. It sought to have measures to ‘ensure a high

em toda a UE”. Neste aspeto, foi a primeira legislação europeia de cibersegurança que, em Portugal, foi vertida para a [lei 46/2018](#).

common level of security of network and information systems across the Union’. In this regard, it was the first European legislation on cybersecurity. In Portugal, it was transposed into [Law No 46/2018](#).



Ecole Polytechnique - Paris - CC BY-SA 2.0

Dois anos depois, a Comissão propôs a sua atualização, o que foi feito com esta NIS 2, “relativa às medidas destinadas a assegurar um elevado nível comum de cibersegurança”, que altera o [regulamento UE 910/2014](#) (sobre identificação eletrónica e serviços de confiança para as transações eletrónicas no mercado interno) e a diretiva UE 2018/1972 ([Código](#)

Two years later, the Commission proposed updating it, which was done with this NIS 2, ‘on measures to ensure a high common level of cybersecurity’. It amends [EU Regulation 910/2014](#) (on electronic identification and trust services for electronic transactions in the internal market) and Directive 2018/1972 ([EU Electronic Communications Code](#)).

[Europeu das Comunicações Eletrónicas](#)).

Por cá, Gameiro Marques, responsável do Centro Nacional de Cibersegurança, já afirmou em público que a transposição da diretiva está a decorrer, devendo o estudo sobre o impacto da NIS 2 estar finalizado até outubro próximo.

A nova diretiva não se aplica às entidades da administração pública quando “exercem as suas atividades nos domínios da segurança nacional, da segurança pública, da defesa ou da aplicação da lei, incluindo a prevenção, investigação, deteção e repressão de infrações penais”. Os bancos centrais e os parlamentos também são excluídos.

Os países podem ainda isentar entidades específicas que exerçam este tipo de atividades em “setores de importância vital como os transportes, saúde, infraestruturas de telecomunicações, [que] estarão agora sujeitos a obrigações adicionais específicas designadamente ao nível das medidas de gestão dos riscos de cibersegurança adotadas. No entanto, a todos será comum a aplicação generalizada de princípios como a segurança by design e a ‘confiança zero’, a capacitação das equipas e, não desprocurando, uma responsabilidade social acrescida ao nível da sensibilização e formação da comunidade em matéria, designadamente, de práticas de ciber-higiene. Tudo isto será

In Portugal, Gameiro Marques, head of the Portuguese National Cybersecurity Centre, has already publicly stated that the directive’s transposition is underway, and the study on the impact of the NIS 2 should be finalised by next October.

The new directive does not apply to public administration entities when they ‘exercise their activities in the domains of national security, public security, defence or law enforcement, including the prevention, investigation, detection and prosecution of criminal offences’. Central banks and parliaments are also excluded.

Countries may also exempt specific entities that carry out this type of activity in ‘vitally important sectors such as transport, health, telecommunications infrastructure, [which] will now be subject to specific additional obligations, namely on the measures of cybersecurity risk management adopted. However, common to all will be the generalised application of principles such as security by design and zero trust, the empowerment of teams and, not less importantly, an increased social responsibility at the level of community awareness and training, namely on cyber hygiene practices. All this will be transversal to the organisations and accompanied by a supervision in terms of compliance’, explains Marta Moreira Dias.



transversal às organizações e acompanhado por uma supervisão em termos de compliance”, explica Marta Moreira Dias.

A diretiva impõe aos Estados a adoção de um quadro estratégico nacional de cibersegurança (Portugal tem essa [estratégia](#) desde 2015, revista em 2019), para estabelecer os recursos necessários e as medidas políticas e regulamentares adequadas a manter um elevado nível de cibersegurança.

No âmbito do documento, “os Estados-Membros devem designar ou criar uma ou várias autoridades competentes responsáveis pela gestão de crises e de incidentes de cibersegurança em grande escala” e designar ou criar um ou vários

The directive requires States to adopt a national cybersecurity strategic framework (Portugal has had this [strategy](#) implemented since 2015, revised in 2019), to establish the necessary resources and the appropriate policy and regulatory measures to maintain a high level of cybersecurity.

Under this document, ‘Member States shall appoint or establish one or more competent authorities responsible for managing large-scale cybersecurity incidents and crises’ and appoint or establish one or more ‘Computer Security Incident Response Teams’ (CSIRT), similar to the [National CSIRT Network](#) in Portugal.

“Computer Security Incident Response Team” (CSIRT), à semelhança da [Rede Nacional de CSIRT](#) em Portugal.

Os países devem depois designar uma destas CSIRT como coordenadora para a divulgação de vulnerabilidades e assim “desempenhar o papel de intermediário de confiança, facilitando, quando necessário, a interação entre a pessoa singular ou coletiva notificadora e o fabricante ou fornecedor de produtos de TIC ou prestador de serviços de TIC que sejam potencialmente vulneráveis, a pedido de qualquer uma das partes”.

A [NIS 2 propõe](#) ainda a criação da European Cyber Crises Liaison Organisation ([EU-CyCLONe](#)), “para apoiar a gestão coordenada de crises e incidentes de cibersegurança em grande escala” e assegurar a troca regular de informação entre instituições, órgãos e organismos da UE.

“Ainda no campo da colaboração interinstitucional, destaca-se o reforço das competências e do âmbito de intervenção da ENISA”, nota Marta Moreira Dias. A cada dois anos, a agência europeia para a cibersegurança deve apresentar ao Parlamento Europeu um relatório sobre o estado da cibersegurança na UE.

Nas medidas de supervisão e execução, quando tiverem “provas, indícios



Countries should then appoint one of these CSIRTs as a vulnerability disclosure coordinator, and thus ‘play the role of trusted intermediary, facilitating, where necessary, interactions between the notifying natural or legal person and the manufacturer or supplier of ICT products or the ICT service provider who are potentially vulnerable, at the request of either party.’

The [NIS 2 also proposes](#) the creation of the European Cyber Crises Liaison Organisation ([EU-CyCLONe](#)), ‘to support the coordinated management of large-scale cybersecurity incidents’ and ensure the regular exchange of information between Member States and Union institutions, bodies and agencies.

‘Also in the field of interinstitutional collaboration, the strengthening of ENISA’s competences and scope of intervention stands out,’ notes Marta Moreira Dias. Every two years, the European Union Agency for

ou informações de que uma entidade importante não está alegadamente a cumprir a diretiva, em especial os seus artigos 21º e 23º, os Estados-Membros devem assegurar que as autoridades competentes atuam em conformidade, se necessário, tomando medidas de supervisão ex post”, que sejam eficazes, proporcionadas e dissuasivas.

Os referidos artigos referem-se respetivamente às medidas de gestão dos riscos de cibersegurança e às obrigações de notificação. Eles são igualmente importantes na aplicação de coimas tanto às entidades essenciais como às importantes.

A NIS 2 classifica as entidades abrangidas pela diretiva, “para efeitos de cumprimento das obrigações relativas às medidas de gestão dos riscos de cibersegurança e à notificação”, em duas categorias: entidades essenciais e importantes, “refletindo a medida em que são fundamentais no que respeita ao seu setor ou ao tipo de serviço que prestam, bem como a sua dimensão”. São os Estados-membros quem estabelece e comunica à Comissão a lista e categoria destas entidades.

No geral, as essenciais têm menos de 250 empregados e um volume de negócios abaixo dos 50 milhões de euros, enquanto as importantes asseguram me-

Cybersecurity should present to the European Parliament a report on the state of cybersecurity in the EU.

In the supervision and enforcement measures, when they have ‘proof, evidence or information that an important entity is allegedly not complying with the directive, namely with Articles 21 and 23 thereof, Member States must ensure that the competent authorities act accordingly, if necessary, by taking effective, proportionate and dissuasive ex post supervisory measures’.

These articles refer to cybersecurity risk management measures and reporting obligations, respectively. They are equally important in the application of fines to both essential and important entities.

The NIS 2 classifies the entities covered by the Directive ‘for the purpose of complying with the cybersecurity risk management measures and notification obligations’, into two categories: essential entities and major entities, ‘reflecting the extent to which they are essential with respect to their industry or the type of service they provide, as well as their size’. The Member States establish and communicate to the Commission the list and category of these entities.

Generally speaking, essential entities have fewer than 250 employees and a

nos de 50 funcionários e um volume de negócios inferior a 10 milhões.

Na vertente da violação de obrigações nos artigos 21º ou 23º, as entidades essenciais podem ser multadas (ver “O panorama das coimas na NIS 2 versus RGPD”). Cabe aos Estados-Membros estabelecerem regras sobre as sanções que “devem ser efetivas, proporcionadas e dissuasivas”, assim como notificar a Comissão Europeia até 17 de janeiro de 2025 dessas regras e das posteriores alterações.

A cada três anos, até 17 de outubro de 2027, a Comissão deve avaliar a aplicação da diretiva e apresentar um relatório ao Parlamento e ao Conselho europeus.

“Esta diretiva europeia vai ajudar cerca de 160 mil entidades a reforçar o seu controlo da segurança e a tornar a Europa um lugar seguro para viver e trabalhar. Permitirá também a partilha de informação com o sector privado e parceiros em todo o mundo. Se estamos a ser atacados à escala industrial, precisamos de responder à escala industrial”, [declarou](#) o eurodeputado Bart Groothuis. “Esta é a melhor legislação de cibersegurança que o continente já viu, porque transformará a Europa no tratamento de ciberincidentes de forma pró-ativa e orientada para os serviços”, acrescentou.

turnover of less than EUR 50 million, while important entities have fewer than 50 employees and a turnover of less than EUR 10 million.

When it comes to breach of obligations pursuant to Articles 21 or 23, essential entities can be fined (see ‘The landscape of fines in NIS 2 vs GDPR’). It is up to Member States to set the rules on sanctions which ‘must be effective, proportionate and dissuasive’. They must also notify the European Commission by 17 January 2025 of these rules and subsequent amendments.

Every three years, until 17 October 2027, the Commission must evaluate the implementation of the directive and report to the European Parliament and Council.

‘This European directive will help around 160 000 entities to strengthen their security monitoring and make Europe a safe place to live and work. It will also allow information sharing with the private sector and partners around the world. If we are being attacked on an industrial scale, we need to respond on an industrial scale’, [said](#) MEP Bart Groothuis. ‘This is the best cybersecurity legislation the continent has yet seen, because it will transform Europe to handling cyber incidents pro-actively and service orientated’ he added.



As coimas: NIS 2 versus RGPD

A NIS 2 introduz coimas que podem chegar a um montante máximo não inferior a 10.000,000€ ou a 2% do volume de negócios anual a nível mundial, no exercício financeiro anterior, da entidade essencial, consoante o montante que for mais elevado. No caso das entidades importantes, as coimas podem chegar a um montante máximo não inferior a 7.000,000€ ou a 1,4% do volume de negócios anual a nível mundial, consoante o montante que for mais elevado.

O RGPD introduziu coimas, nos casos menos graves, que podem ter um valor até 10.000,000€ ou 2% do volume de negócios anual a nível mundial, consoante o montante que for mais elevado, e nos casos mais graves, as coimas podem ter um valor até 20.000,000€ ou 4% do volume

The fines: NIS 2 vs GDPR

The NIS 2 introduces fines, for essential entities, up to a maximum of no less than €10 000 000 or 2 % of the annual worldwide turnover from the preceding financial year, whichever is higher. For important entities, fines can reach up to a maximum of no less than €7 000 000 or 1.4 % of the annual worldwide turnover, whichever is higher.

For minor cases, the GDPR has introduced fines up to €10 000 000 or 2 % of annual worldwide turnover, whichever is higher, and for more serious cases, fines up to €20 000 000 or 4 % of the annual worldwide turnover, whichever is higher.

In Portugal, with Law No 58/2019, the sanctioning frameworks were adapted, being applicable to public and private

de negócios anual a nível mundial, consoante o montante que for mais elevado.

Em Portugal, com a Lei n.º 58/2019, as molduras sancionatórias foram adaptadas, sendo aplicáveis a entidades públicas e privadas, e variando em função da dimensão (empresarial) do infrator, prevendo-se critérios de ponderação na determinação da coima a aplicar, sendo introduzidos valores mínimos de 5 000€ no caso de contraordenações muito graves e 2 500€ para contraordenações graves de grandes empresas. Os valores mínimos das pequenas e médias empresas oscilam entre 1 000€ e 2 000€ respetivamente e entre 1 000€ e 500€ para pessoas singulares.

Um aspeto distintivo fundamental entre o RGPD e a NIS 2 é o facto desta, por regra, não ser aplicável a micro e pequenas empresas, embora com exceções como com os registries de TLDs. No entanto, a NIS 2 alerta para a necessidade da Comissão Europeia fornecer orientações sobre a aplicação dos critérios relativos às microempresas e às pequenas empresas para avaliar se elas são abrangidas pelo âmbito da presente diretiva, portanto esta realidade poderá sofrer alterações.

Há um aumento dos setores abrangidos pela NIS 2, portanto, mais entidades sujeitas à aplicação de coimas. Umas terão

entidades; they vary according to the (business) size of the offender, providing for weighting criteria in determining the fine to be applied, with minimum amount of €5 000 being introduced for very serious administrative offences and €2 500 for serious administrative offences by large companies. The minimum amounts range from €1 000 to €2 000 for small- and medium-sized companies respectively and from €1 000 to €500 for natural persons.

A key distinguishing feature between the GDPR and the NIS 2 is that, as a rule, the later does not apply to micro and small businesses, although there are exceptions such as TLD registries. However, NIS 2 alerts to the need for the European Commission to provide guidance on the application of the criteria for micro and small enterprises to assess whether they fall within the scope of this directive, which means that this reality may change.

There is an increase in the number of sectors covered by the NIS 2, meaning that there could be more entities subject to the application of fines. Some will be more financially robust than others. These are different realities, as well as the socio-economic reality of essential/important entities between European countries, so the impact that fines will have will also be different.

mais robustez financeira do que outras. São realidades díspares, assim como a realidade socio-económica de entidades essenciais/importantes entre países europeus, pelo que o impacto das multas será também diferente.

Será importante avaliar se vão estar criadas as condições para o exercício da atividade sancionatória (enforcement), que passa pela capacidade de desenvolver processos de averiguações prévios altamente alocadores de recursos;

As coimas, que não estavam tipificadas na NIS e são agora trazidas pela NIS 2, têm um manifesto efeito dissuasor, mas que pode ser pernicioso se pensarmos que o nosso tecido empresarial ainda não se move propriamente numa cultura de cibersegurança.

Tão importante como as coimas é a questão reputacional. As falhas de segurança que veem a público, com ou sem impacto real, minam, muitas vezes de forma irreduzível, a confiança dos consumidores e dos pares, e as consequências que daí advêm são óbvias.

Em suma, as entidades portuguesas estão tão preparadas para estas coimas como estavam (e estão) para as resultantes do incumprimento do quadro legal aplicável à privacidade e proteção de dados (RGPD + Lei 58/2019). As di-

It will be important to assess whether the conditions for enforcement of sanctions will be created, which includes the ability to develop prior investigation processes that allocate a large number of resources;

Fines, which were not typified in the NIS and are now brought to light by the NIS 2, have a clear dissuasive effect, which may be pernicious if we think that our business fabric is not yet moving properly in a culture of cybersecurity.

Just as important as fines is the issue of reputation. The security flaws that come to light, with or without real impact, undermine, often irreducibly, the trust of consumers and peers, and the consequences are obvious.

In short, Portuguese entities are as prepared for these fines as they were (and are) for those resulting from non-compliance with the legal framework applicable to privacy and data protection (GDPR + Law No 58/2019). The immediate differences here will be the scope of application (broader in the GDPR) and, above all, the control - or lack thereof - of the acts, diligences or omissions leading to the possible application of a fine or penalty. It seems to be more difficult for a company to obviate an external attack, highly sophisticated and without apparent trace, than to internally

Coimas da CNPD

Em cinco anos, a Comissão Nacional para a Proteção de Dados (CNPD) aplicou 230 sanções, assim distribuídas:

- 2018 – 50 coimas num total de €80 000
- 2019 – 34 coimas (€600 000)
- 2020 – 15 coimas (€47 000)
- 2021 – 60 coimas (€1 491 500)
- 2022 – 71 coimas (€4 802 000, com a maior de sempre, no valor de €4.3M, ao INE num cúmulo jurídico de cinco contraordenações)

Total: €7 020 500

CNPD Fines

In five years, the National Data Protection Authority (CNPD) applied 230 sanctions, distributed as follows:

- 2018 – 50 fines totalling €80 000
- 2019 – 34 fines (€600 000)
- 2020 – 15 fines (€47 000)
- 2021 – 60 fines (€1 491 500)
- 2022 – 71 fines (€4 802 000, the largest ever, totalling €4.3M, to INE in a legal cumulation of five administrative offences)

Total: €7 020 500

ferenças imediatas aqui serão o âmbito de aplicação (mais alargado no RGPD) e, sobretudo, no controlo – ou falta dele – dos atos, diligências ou omissões conducentes à eventual aplicação de uma coima ou multa. Parece ser mais difícil para uma empresa obviar a um ataque externo, altamente sofisticado e sem rasto aparente, do que propriamente fazer cumprir internamente as regras e procedimentos decorrentes do RGPD, o que não sendo tarefa fácil está menos condicionada por fatores exógenos não controláveis.

Marta Moreira Dias (Board of Directors .PT)

enforce the rules and procedures arising from the GDPR – which, not being an easy task, are less conditioned by non-controllable exogenous factors.

Marta Moreira Dias (Board of Directors .PT)



Denúncias de cibercrime continuam a aumentar

O Gabinete Cibercrime da Procuradoria-Geral da República registou novamente um acréscimo de denúncias de cibercrimes em 2022. As denúncias têm vindo a aumentar de forma “regular, constante e persistente”. De 2021 para 2022, aumentaram 73,5%.

O phishing foi o crime mais denunciado (358 casos), seguindo-se as burlas online e com páginas Web falsas, no mercado imobiliário, fraudes em plataformas de vendas online e em apps de pagamentos, com criptoativos ou o fenómeno conhecido como “olá mãe, olá pai” e a “CEO fraud”.

Mais ataques a dados de menos pessoas

O número de dados pessoais comprometidos em 2022 nos EUA ultrapassou o total de 1800 casos, afetando mais de 422 milhões de indivíduos. Estes acessos não autorizados a dados sensíveis devem-se a incidentes de violações de dados, fugas de dados ou exposição dos mesmos.

Reports of cybercrime continue to rise

The Cybercrime Office of the Prosecutor General’s Office recorded another increase in cybercrime-related reports in 2022. These reports have been growing at a ‘regular, constant and persistent’ pace. From 2021 until last year, increased by 73.5 %.

Phishing was the most reported crime (358 cases), followed by online scams and scams with ‘fake’ web pages, in the real estate market, fraud in online sales platforms and payment apps, scams with cryptoassets or the phenomenon known as ‘Hi Mum and Dad’ and the ‘CEO fraud’.

More attacks on fewer data holders

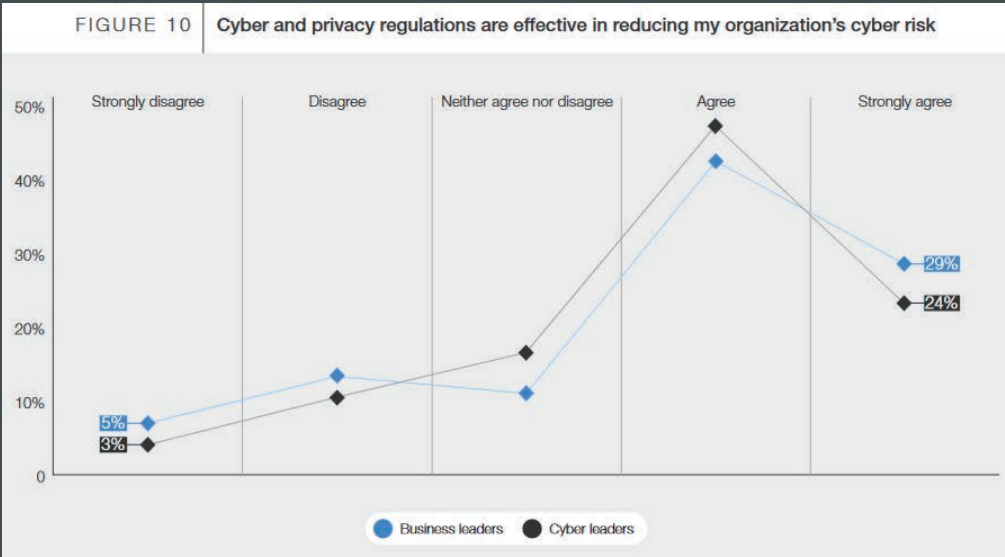
The number of personal data compromised in 2022 in the US exceeded 1800 total cases, affecting more than 422 million people. These unauthorised accesses to sensitive data originate from incidents of data breaches, data leaks or data exposure.

Gestores mais conscientes das ciberameaças?

Os líderes de negócio estão mais atentos às ciberameaças do que em anos anteriores, mas as consequências dessa atenção não são visíveis de forma significativa nas organizações, constata o [2023 Global Cybersecurity Outlook](#).

Managers more aware of cyberthreats?

Business leaders are more aware of cyberthreats than in previous years, but the consequences of that attention are not significantly visible in organisations, finds the [2023 Global Cybersecurity Outlook](#).



Apesar de estarem disponíveis para lidar com os ciber-riscos apontados pelos responsáveis de segurança informática - como a interrupção do negócio ou os danos reputacionais -, “concordar sobre a melhor forma de abordar o ciber-risco continua a ser um desafio para os líderes organizacionais”. Mesmo com 43% deles a considerar provável que a sua organização pode sofrer um ciberataque nos próximos dois anos.

Despite being willing to deal with the cyber risks pointed out by cybersecurity officers - such as business disruption or reputational damage - ‘agreeing on how best to address cyber risk remains a challenge for organisational leaders’. Even with 43 % of them considering it likely that their organisation could suffer a cyberattack within the next two years.

3



Marta Moreira Dias

Board of Directors .PT
Board of Directors .PT

1. Quais as alterações mais marcantes entre as diretivas NIS e NIS 2?

Partimos de um ambicioso horizonte comum: uma europa mais segura, mais forte e resiliente em matéria de cibersegurança. Numa visão puramente holística, diria ser esta a essência de ambos os diplomas.

A ideia de mobilização generalizada dos estados-membros para a preparação e implementação de estratégias nacionais de cibersegurança, assentes em princípios de forte colaboração do ponto de vista nacional e internacional e a perceção de que as matérias da segurança devem ter uma abordagem transnacional e de alargada horizontalidade sectorial, são bases comuns de dois instrumentos de fonte comunitária que distam entre si sete anos, e que são parte de um já longo pipeline legislativo da regulação do espaço digital europeu.

A Diretiva NIS, transposta a nível nacional pela Lei n.º 46/2018, teve o mérito in-

1. What are the most striking changes between the NIS and NIS 2 directives?

We start from a common ambitious horizon: a more secure, stronger and resilient Europe in terms of cybersecurity. In a purely holistic view, I would say this is the essence of both pieces of legislation.

The idea of generalised mobilisation of the member states for the preparation and implementation of national cybersecurity strategies, based on principles of strong collaboration from a national and international point of view, and the perception that security issues should have a transnational approach and a wide sectoral horizontality are the common bases of two community-source instruments that are seven years apart and included on an already long legislative pipeline of regulation on the European digital space.

The NIS Directive, transposed into national legislation by Law No 46/2018, had the undeniable merit of contributing to alerting to the impact and need to address issues on network security and information systems, reinforcing their normative dignity. With that, a path of changing mentalities began to take shape, followed by a timid, but also costly, reinforcement of internal infrastructures, training of teams, implementation of security operation centres - of which the PTSOC is an example of -, and creation of cooperation groups and network of national computer

defetível de contribuir para alertar para o impacto e necessidade do tratamento das matérias de segurança dos sistemas de rede e informação, reforçando-lhes a dignidade normativa. Com isso, foi iniciado um caminho de mudança de mentalidades – onde tudo começa –, ao qual se seguiu um tímido, porque também dispendioso, reforço de infraestruturas internas, de capacitação de equipas, a implementação de centros de operação de segurança – de que é exemplo o PTSOC –, e a criação de grupos de cooperação e de rede de equipas nacionais de resposta a incidentes de segurança informática (CERTs, CSIRTs, etc.).

Com os desafios a que todos fomos e continuamos sujeitos, entre 2016 e 2023 os ataques de cibersegurança aumentaram exponencialmente em volume, sofisticação e impacto, a resiliência e preparação de pessoas, empresas e Estado revelou-se insuficiente e com falhas facilmente exploradas. Acresce a falta de uma estratégia comum, dialogante e eficaz de resposta a mais esta guerra. Hoje, o estágio de evolução, as expectativas e o impacto são diversos, estamos todos vários degraus acima, há uma curva de aprendizagem que deve ser observada e entendida. É maioritariamente esse o grande desafio a que a NIS 2 quer dar resposta.

Partimos, portanto, da identificação dos pontos de interceção entre ambas as diretivas, percebemos o racional subjacente ao processo que presidiu a revisão da NIS, e de

security incident response teams (CERTs, CSIRTs, etc.).

Between 2016 and 2023, taking into account the challenges we have all been and continue to be subjected to, cybersecurity attacks increased exponentially in volume, sophistication and impact; the resilience and preparation of people, companies and the State proved to be insufficient, with their flaws being easily exploited. Adding to it is the lack of a common, dialoguing and effective strategy to respond to this war. Today, the stage of evolution, the expectations and the impact are diverse. We are all several steps up. There is a learning curve that must be observed and understood. This is, in short, the major challenge the NIS 2 wants to address.

We start by identifying where both directives intersect, understanding the rationale behind the process which presided over the revision of the NIS, and which resulted in the publication of the NIS 2. Let us now look at those which are the most striking changes between both diplomas, especially under the lens of the .pt top level domain name registry.

Five major changes can be immediately identified: broadening of the subjective scope of application, namely at sectoral level; risk management-oriented approach, with a focus on prevention and mitigation, therefore going beyond purely reactive measures (accompanied by new reporting obligations); responsibility of the management bodies of

onde resultou a publicação da NIS 2. Olhe-mos agora para aquelas que são as alterações mais marcantes entre ambos os diplomas, especialmente sob a lente do registo de nome de domínio de topo .pt.

No imediato identificam-se cinco grandes alterações: alargamento do âmbito subjetivo de aplicação, nomeadamente a nível sectorial; abordagem orientada à gestão do risco, com enfoque na prevenção e mitigação indo, portanto, além das medidas puramente reativas (acompanhada com novas obrigações de reporte); responsabilidade dos órgãos de gestão das empresas e organizações; reforço do papel da colaboração; e, por fim, sob o manto inspiracional do RGPD, definição clara de um quadro contraordenacional pesado.

O alargamento do âmbito e dos sectores abrangidos pela NIS 2 implica que mais organizações terão de abordar e tratar formalmente o tema da cibersegurança, sendo efetuada uma distinção entre “entidades essenciais” e “entidades importantes”. Para além da questão semântica, são residuais as diferenças entre ambas as categorias. Destaca-se o facto de, em relação às primeiras, a supervisão poder ser realizada *ex ante* (a título preventivo) e *ex post* (pós verificação de um incidente). Para as entidades importantes, a supervisão será feita apenas *ex post*.

O .PT, hoje qualificado à luz da NIS, e subsequentemente da Lei n.º 46/2018, como operador de serviços essenciais assumirá a

companies and organisations; reinforcement of the role of collaboration; and, finally, under the inspirational mantle of the GDPR, clear definition of a burdensome administrative offence framework.

Broadening the scope and the sectors covered by the NIS 2 implies that more organisations will have to formally address and deal with the issue of cybersecurity, with a distinction being made between ‘essential entities’ and ‘important entities’. Beyond semantics, the differences between both categories are residual. We highlight the fact that, for the former, supervision can be carried out *ex ante* (preventively) and *ex post* (after an incident has occurred). For important entities, supervision will only be carried out *ex post*.

The .PT, today qualified under the NIS, and subsequently under Law No 46/2018, as an operator of essential services, will take on the nature of an essential entity. This categorisation is accompanied by another, equally new one, that of ‘critically important sectors’ and ‘other critical sectors’. How an entity is classified in either one of these sectors is independent of its qualification as an essential or an important entity.

The .PT, as a Top Level Domain Name (TLD) registry, will be considered a critically important sector integrated in the digital infrastructures. Focusing on the TLDs and their registrars, new obligations gain

natureza de entidade essencial. Esta categorização vem acompanhada de uma outra, igualmente nova, a de “sectores de importância crítica” e “outros sectores críticos”. O enquadramento de uma entidade num destes sectores é independente da sua qualificação como entidade essencial ou importante.

O .PT, na qualidade de registo de nome de domínio de topo (TLD), vai passar a enquadrar-se como sector de importância crítica integrado nas infraestruturas digitais. Descendo o foco aos TLD e aos seus registrars, novas obrigações ganham eco normativo. Referimo-nos em concreto às que decorrem da gestão da base de dados WHOIS, importante ferramenta sobretudo para ações de investigação criminal e, por isso, capazes de contribuir para o chamado elevado nível comum de cibersegurança em toda a UE. Aqui emergem pesadas obrigações de recolha, verificação, monitorização e disponibilização de contactos associados aos responsáveis dos nomes de domínios, que, numa análise crítica, vão ao arrepio do cumprimento de regras de proporcionalidade e de minimização de dados que emergem como princípios basilares do RGPD.

A NIS 2 estende o seu âmbito de aplicação territorial a entidades que não estando sediadas no espaço europeu prestam os seus serviços nesta circunscrição. Se, mais uma vez, vemos os TLD europeus a cair numa malha acrescida de regras que não são comuns às restantes mais de 1 000 entidades que

normative echo. We refer specifically to those arising from the management of the WHOIS database, an important tool geared towards criminal investigations, therefore capable of contributing to the so-called high common level of cybersecurity throughout the EU. Heavy obligations of collection, verification, monitoring and provision of contacts associated with those responsible by domain names emerge which, in a critical analysis, go against the compliance with proportionality and data minimisation rules that emerge as basic principles of the GDPR.

The NIS 2 extends its territorial scope of application to non-EU based entities that still provide their services therein. If, once again, we see European TLDs falling under an increasing mesh of rules not common to the other more than 1000 entities that compete with them daily, at least this safeguard seems to mitigate, even if residually, that same imbalance.

Prioritising cybersecurity at the level of leadership is another innovation vector of the NIS 2. An example of this is top management's accountability for identified non-conformities regarding the adoption of cybersecurity risk management measures and the obligation to provide training and capacity building in the area.

We hope that the NIS 2, and especially its transposition into national legislation, becomes an instrument that generates more

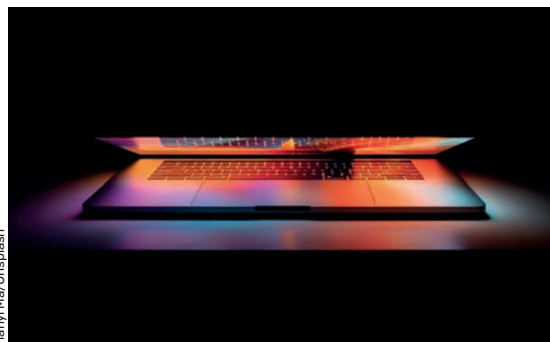
com eles diariamente concorrem, pelo menos esta salvaguarda parece atenuar, ainda que residualmente, esse mesmo desequilíbrio.

Priorizar a cibersegurança ao nível da liderança, é outro vetor de inovação da NIS 2. Espelho disso é a responsabilização da gestão de topo pelas inconformidades identificadas relativamente à adoção das medidas de gestão dos riscos de cibersegurança e a própria obrigação de formação e capacitação na área.

Esperamos que a NIS 2, e sobretudo a transposição para a ordem jurídica nacional, venha a constituir-se como um instrumento gerador de mais confiança e segurança jurídica para os cidadãos, empresas e organizações em geral e que tenha a virtude de controlar esta escalada que diariamente belisca a segurança das nossas redes e sistemas e que se afigura altamente inibidora da inovação, da liberdade de circulação de dados e ideias e potenciadora de uma internet fragmentada.

2. O novo quadro regulatório parece ter menos regras do que a NIS, mas há realmente uma simplificação nas regras?

A NIS 2 vem claramente reforçar o standard de medidas aplicáveis em matéria de cibersegurança e que estavam já cristalizadas a nível nacional em dois diplomas centrais, a Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço, e o Decreto-Lei n.º 65/2021



Tianyi Ma/Unsplash

confidence and legal security for citizens, companies and organisations in general; that has the virtue of controlling this escalation that, everyday, pinches the security of our networks and systems, and that seems to highly inhibit innovation, the free movement of data and ideas and enhance a fragmented internet.

2. The new regulatory framework seems to have fewer rules than the NIS, but is there really a simplification in the rules?

The NIS 2 clearly reinforces the standard of measures applicable to cybersecurity which were already crystallised at national level in two central pieces of legislation, Law No 46/2018 of 13 August, which establishes the legal regime for cyberspace security, and Decree-Law No 65/2021, which regulates the Cyberspace Security Legal Framework and defines the obligations on cybersecurity certification by implementing Regulation (EU) 2019/881 of the European Parliament.

In parallel, and in addition to various

que regulamenta o Regime Jurídico da Segurança do Ciberespaço e define as obrigações em matéria de certificação da cibersegurança em execução do Regulamento (UE) 2019/881 do Parlamento Europeu.

Paralelamente, e para além de diversa legislação avulsa, há diretrizes e boas práticas emanadas de fonte diversa como são, a título de exemplo, as recentes [“Technical Guideline: Security Measures for Top-Level-Domain Name Registries”](#), do NIS Cooperation Group, recomendações diversas emitidas pela ENISA e, dentro fronteiras, a Diretriz/2023/1 da CNPD no âmbito do RGPD [“Sobre medidas organizativas e de segurança aplicáveis aos tratamentos de dados pessoais”](#), assim como os [guias e recomendações técnicas](#) produzidos pelo Centro Nacional de Cibersegurança.

Não estamos claramente numa situação de vazio legal, num espaço de ninguém, onde se impusesse um novo ou diametralmente oposto quadro normativo.

A auscultação realizada aos Estados Membros da NIS revelou, nas palavras do legislador comunitário, “deficiências intrínsecas que a impedem de responder de forma eficaz a desafios atuais e emergentes no domínio da cibersegurança”. Se tivermos presente que o ciberespaço, para além da sua natureza transnacional, capaz de desafiar qualquer princípio de territorialidade ou de soberania nacional, é uma realidade dinâmica, cada vez mais complexa e em constante mutação,

separate legislation, there are several guidelines and good practices from various sources, such as, by way of example, the recent [‘Technical Guideline: Security Measures for Top-Level-Domain Name Registries’](#), by the NIS Cooperation Group and various recommendations issued by ENISA. Domestically, there is also the CNPD’s Guideline/2023/1 under the GDPR [‘On organisational and security measures applicable to the processing of personal data’](#), and other [technical guides and recommendations](#) by the Portuguese National Cybersecurity Centre.

We are clearly not in a situation of legal vacuum, in a no man’s space, where a new or diametrically opposed regulatory framework would be imposed.

The consultation conducted with NIS Member States showed, in the words of the EU legislator, ‘intrinsic weaknesses that prevent it from responding effectively to current and emerging cybersecurity challenges’. If we bear in mind that cyberspace, in addition to its transnational nature, capable of challenging any principle of territoriality or national sovereignty, is an increasingly complex and constantly changing dynamic reality, we can easily understand the difficulty of creating a legislative edifice with fewer and simpler rules. In truth, our reservations are attenuated when we realise that there was, for example, a concern to simplify the communication of

facilmente percebemos a dificuldade de criar um edifício legislativo com menos e mais simples regras. Em boa verdade, as nossas reservas atenuam-se ao verificar que houve uma preocupação em, por exemplo, simplificar a comunicação de informações e adotar mecanismos de comunicação automática e direta, ou em promover o uso de ferramentas de código aberto, que tendencialmente podem facilitar a interoperabilidade entre as ferramentas de segurança, ou estimular a cooperação para, designadamente, facilitar a divulgação coordenada de vulnerabilidades, otimizando tempo e recursos.

Numa análise mais fina, chegamos a um ponto sem retorno onde o objetivo de promoção de um ciberespaço mais seguro, aberto e resiliente, esbarrou, literalmente, num leque exaustivo e desproporcionado de obrigações que nada têm de simples.

Olhemos para dois casos concretos, parte do ecossistema de registo de domínios: os TLD – por exemplo, o .pt – e os prestadores de serviços de DNS – por exemplo, um agente de registo (registrar) – para além do cumprimento estrito de novas medidas de gestão dos riscos de cibersegurança, tipificadas no artigo 21.º, até 17 de outubro de 2024, a Comissão deve adotar atos de execução que estabeleçam requisitos técnicos e metodológicos a eles associados, e que deverão ser objeto de cumprimento estrito. Mas reitera-se, em especial para os TLD, que o caminho não foi o da simplificação. Porém, e em abono da verdade, as

information, to adopt automatic and direct communication mechanisms, to promote the use of open source tools, as they tend to facilitate interoperability between security tools, or to stimulate cooperation, namely in order to facilitate the coordinated disclosure of vulnerabilities, optimising time and resources.

Under a more detailed analysis, we have reached a point of no return where the goal of promoting a more secure, open and resilient cyberspace has literally collided with an exhaustive and disproportionate range of obligations that are anything but simple.

Let us look at two specific cases, part of the domain registration ecosystem: the TLDs – for example, .pt – and DNS service providers – for example, a registrar. In addition to strict compliance with new cybersecurity risk management measures, typified in Article 21, by 17 October 2024 the Commission must adopt implementing acts that establish technical and methodological requirements associated with them, which should be subject to strict compliance. But it is reiterated, particularly for TLDs, that the path has not been one of simplification. However, and in all truth, the obligations that now derive from Article 28 [on the domain name registration database] resulted from a long and highly debated negotiation process.

Let us not forget the Opinion of the European Data Protection Supervisor on this

obrigações que decorrem hoje do artigo 28.º [sobre a base de dados relativos ao registo dos nomes de domínio] resultaram de um processo negocial longo e altamente debatido.

Relembre-se o Parecer da Autoridade Europeia para a Proteção de Dados a este propósito sobre este artigo, muito em linha com o posicionamento dos registries europeus materializado no comentário público do CENTR, onde se alertava para a importância da clarificação de conceitos como “informação relevante” e pedido “lícito e devidamente justificado” e, sobretudo, para o facto do RGPD, per si, já conceder a devida tutela aos dados pessoais, nomeadamente os que são tratados no WHOIS.

A NIS 2 veio trazer obrigações adicionais aos TLD e registrars, que devem recolher e manter dados exatos e completos relativos ao registo de nomes de domínio, numa base de dados específica, com a devida diligência, e em conformidade com o direito da UE em matéria de proteção de dados. Este tratamento de dados constitui uma obrigação jurídica na aceção do RGPD. Mas o legislador comunitário foi mais longe e, inclusivamente, elencou a tipologia de dados que deve ser tratada - muito para além do que acontece hoje - impondo aos TLD que disponham de políticas e procedimentos de verificação, e mecanismos céleres de disponibilização de informação solicitada neste âmbito sem demora injustificada e, em qualquer caso, no prazo de 72 horas a contar da receção dos

article, very much in line with the position of European registries materialised in CENTR’s public comment which alerted to the importance of the clarification of concepts such as ‘relevant information’ and ‘lawful and duly justified’ request and, above all, to the fact that the GDPR, per se, already grants due protection to personal data, namely those processed in the WHOIS.

The NIS 2 brought additional obligations for TLDs and registrars to collect and maintain accurate and complete domain name registration data in a dedicated database with due diligence and in compliance with EU data protection law. This data processing constitutes a legal obligation within the meaning of the GDPR. But the EU legislator has gone further and even listed the types of data that must be processed - far beyond what happens today - requiring TLDs to have verification policies and procedures in place, as well as rapid mechanisms to make information requested in this context available without undue delay and, in any case, within 72 hours of receiving access requests. Less rules and more simplification? The peremptory answer from a TLD can only be one: no.

3. How do you anticipate the application of the NIS 2 in Portugal, what are the potential problems and challenges?

For the NIS 2 directive to take effect at national level, Portugal must adopt a law

pedidos de acesso. Menos regras e mais simplificação? A resposta perentória de um TLD não pode ser outra: não.

3. Como antecipa a aplicação da NIS 2 em Portugal, quais os potenciais problemas e desafios?

Para que a diretiva NIS 2 produza efeitos a nível nacional, Portugal tem de adotar uma lei com vista à sua transposição, devendo tal acontecer até 17 de outubro de 2024. Por regra, as diretivas só produzem efeitos após a sua transposição.

No entanto e desde logo acautelando eventuais atrasos nos processos legislativos internos, o Tribunal de Justiça da União Europeia tem vindo a considerar que uma diretiva que não foi objeto de transposição possa produzir diretamente efeitos na ordem jurídica interna. Neste pressuposto, e de resto à semelhança do que aconteceu com a transposição da NIS, teremos de aguardar aquelas que sejam as opções de harmonização do legislador nacional e esperar que o processo de transposição seja já, ele próprio, inspirado no princípio de colaboração interinstitucional tão enfatizado no articulado da própria Diretiva.

Caberá ainda ao Estado, na própria letra da diretiva, “salvaguardar a funcionalidade e a integridade da Internet e promover a segurança e a resiliência do DNS”, garantir que as partes interessadas pertinentes, nomeadamente as entidades do setor privado da UE,

with a view to its transposition, which must happen by 17 October 2024. As a rule, directives only take effect after their transposition.

However, already anticipating possible delays in internal legislative procedures, the Court of Justice of the European Union has been considering that a directive that has not yet been transposed may have direct effect in the internal legal order. Under this assumption, and similarly to what happened with the transposition of the NIS, we will have to wait for the harmonisation options of the national legislator and hope that the transposition process itself is already inspired by the principle of interinstitutional collaboration so emphasised in the articles of the Directive itself.

It is also up to the State, in the very letter of the Directive itself, to ‘safeguard the functionality and integrity of the Internet and promote the security and resilience of the DNS’, to ensure that relevant stakeholders, including EU private sector entities, are encouraged to adopt a strategy to diversify the DNS resolution, as well as a European, public and secure DNS resolution service. This is obviously a matter close to .PT’s heart.

The NIS 2 also entrusts the national legislator to set up a system providing for effective, proportionate and dissuasive sanctions, for example, in cases of serious infringements.

sejam incentivados a adotar uma estratégia de diversificação da resolução do DNS, assim como de um serviço europeu, público e seguro de resolução do DNS. Matéria que obviamente é cara ao .PT.

A NIS 2 remete ainda para o legislador nacional a criação de um sistema que preveja sanções efetivas, proporcionadas e dissuasivas nos casos, por exemplo de infrações graves.

Também a vigente Estratégia Nacional de Segurança do Ciberespaço (2019-2023) terá de ser revisitada no sentido de, nomeadamente, reforçar as políticas de promoção da ciberproteção ativa como parte de uma estratégia defensiva mais ampla e repensar políticas eficazes de resposta ao aumento dos ataques de ransomware. Também neste campo são identificadas ações a desenvolver e implementar a nível nacional.

Figura interessante trazida pela NIS 2 para a área da cibersegurança é a criação de parcerias público-privadas (PPP) para fins de troca de conhecimentos, alertas, exercícios em matéria de ciberameaças e de incidentes, gestão de crises e partilha de boas práticas.

Outro grande desafio será garantir que pessoas, empresas e Estado estão adequadamente equipados, em termos de capacidade técnica e organizativa, para evitar, detetar, enfrentar e atenuar os incidentes e os riscos. Sendo que, ao lado de uma infraestrutura técnica reforçada, deverá estar sempre

The current National Strategy for Cyberspace Security (2019-2023) will also need to be revisited in order to, inter alia, strengthen policies promoting active cyber protection as part of a broader defensive strategy and to rethink effective policies to respond to the increase in ransomware attacks. Also in this field, actions to be developed and implemented at national level are identified.

An interesting figure brought by the NIS 2 into the area of cybersecurity is the creation of public-private partnerships (PPP) to exchange knowledge, alerts, exercises on cyberthreat and incident, crisis management and sharing of best practices.

Another major challenge will be to ensure that people, companies and the state are adequately equipped, in terms of technical and organisational capacity, to prevent, detect, address and mitigate incidents and risks. Alongside a reinforced technical infrastructure, there should always be a team duly trained and prepared to mitigate and treat, and above all, to prevent and anticipate the growing sophistication of cyberthreats. All this comes at a cost and will have a serious impact on the budgets of the entities covered. The anticipated framework of administrative offences and the level and impact of the responsibility of management bodies will probably lead to the demand for civil liability insurance in the area of cybersecurity'.

uma equipa devidamente capacitada e preparada para mitigar e tratar, e, sobretudo, prevenir e antecipar a crescente sofisticação das ciberameaças. Tudo isto tem custos e vai ter um impacto sério nos orçamentos das entidades abrangidas. O quadro contraordenacional previsto e o nível e impacto da responsabilidade dos órgãos de gestão, provavelmente vai conduzir à procura de seguros de responsabilidade civil na área da cibersegurança.

Muitos outros desafios se perspetivam. Deixava um último que tem a ver com o enforcement, em concreto a importância de serem definidos mecanismos e competências efetivos, acompanhados dos necessários recursos para controle e monitorização da aplicação da lei, das boas práticas e das diretrizes que derivem da NIS 2.

Em suma, antecipam-se desafios mais do que problemas. Estou confiante que o novo quadro legal, completo com a transposição da NIS 2, poderá contribuir decisivamente para um ciberespaço mais seguro, aberto e resiliente. Como representante do .PT, que pela sua natureza jurídica será fortemente impactado com as novas regras e obrigações da NIS 2, fica um sentimento de expectativa, aliada a um elevado comprometimento e sentido de responsabilidade.

Many other challenges lie ahead. I would like to mention one last challenge, which has to do with enforcement, specifically the importance of defining effective mechanisms and competencies, accompanied by the necessary resources to control and monitor the application of the law, good practices and guidelines that derive from the NIS 2.

In short, challenges rather than problems are anticipated. I am confident that the new legal framework, complete with the transposition of the NIS 2, may contribute decisively to a more secure, open and resilient cyberspace. As a representative of .PT, which by its legal nature will be strongly impacted by the new rules and obligations of the NIS 2, I am left with a feeling of expectation, together with a high commitment and sense of responsibility.



Carlos Cabreiro

Diretor da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), Polícia Judiciária
Director of the National Unit to Combat Cybercrime and Technological Crime (UNC3T), Portuguese Criminal Police

Ransomware, um “crime informático puro”

Ransomware é a terminologia usada para nos referirmos a um programa de computador, especificamente desenhado para infetar os sistemas informáticos, sejam eles servidores, computadores ou terminais de comunicações móveis. Trata-se de um tipo de software que faz parte da categoria dos programas maliciosos, ou malware, e concretiza-se com a cifragem parcial ou total dos dados e informação que o utilizador tem nos seus equipamentos.

Com o acesso restringido, e pese embora o sistema informático continuar a funcionar, é transmitida uma mensagem/alerta ao utilizador que o informa que os seus dados estão controlados pelo atacante, estão bloqueados e inacessíveis, e que a menos que uma determinada quantia seja paga (o “ransom” ou resgate), o acesso aos mesmos não será restabelecido, perdendo toda a sua informação. O montante exigido é variável e é requerido que seja pago em moeda eletrónica, por exemplo em bitcoins.

Estamos, pois, a falar de um cibercrime, um ataque que envolve, percorre e termina

Ransomware, a ‘pure computer crime’

Ransomware is the terminology used to refer to a computer program specifically designed to infect computer systems, be they servers, computers or mobile communication terminals. It is a type of software that belongs to the category of malicious programs (malware), and works by partially or totally encrypting the data and information a given user has on their equipment.

With restricted access, and although the computer system continues to function, a message/alert is sent to the user informing them that their data is now being controlled by the attacker, that said data is blocked and inaccessible, and that unless a certain amount is paid (the ransom), access to it will not be re-established, and all their information will be lost. The amount required is variable and is required to be paid in electronic currency, for example in bitcoins.

We are, therefore, talking about a cybercrime, an attack that encompasses, goes through and ends in the cycle of information, processing and communication technologies (ICT). It is considered a pure

no ciclo das tecnologias de informação, processamento e comunicação (TIPC). É aliás considerado um crime informático puro, porque afeta e compromete de forma decisiva pelo menos dois princípios da segurança da informação: a integridade e a disponibilidade da informação e dos dados do utilizador.

Da forma como nos é apresentado, não nos restam dúvidas que estamos perante um crime de motivação patrimonial que pretende gerar um proveito económico ao criminoso, já que o utilizador do sistema é confrontado com uma mensagem de teor informativo, que lhe exige um pagamento. No entanto, não é desprezível considerar outras motivações que se possam associar ao ego ou ressentimento do atacante, a efeitos concorrenciais, ou mesmo a atuações com motivações ofuscadas, de ordem política e/ou estatal.

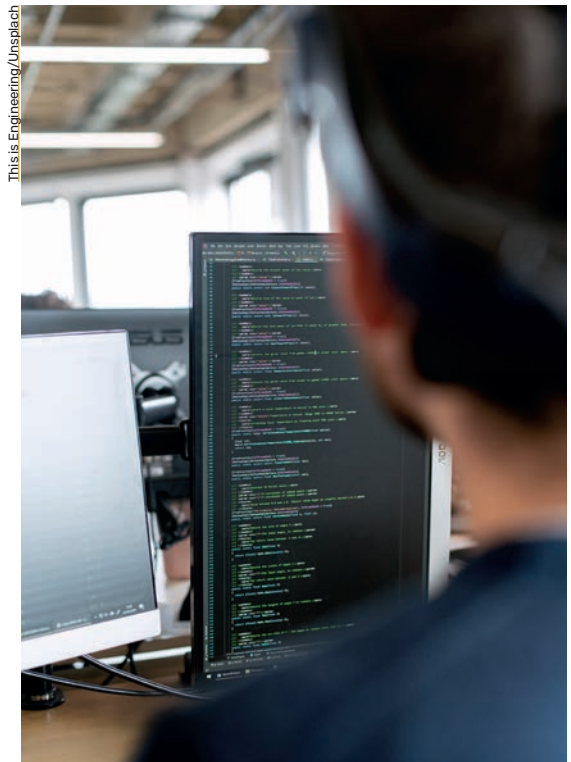
Não pagar

A decisão sobre o não pagamento do resgate parece-nos evidente:

- nunca teremos a certeza de que se obtém a chave de decifragem;
- a lógica do atacante é potenciar o lucro da atividade criminosa, exponenciado a possibilidade de extorquir, mais e mais, e aumentar o proveito económico;
- o “modus operandi” é suscetível de uso e promovido pelo crime organizado, por isso, não podemos garantir o seu financiamento.

computer crime because it decisively affects and compromises at least two principles of information security: the integrity and availability of user information and data.

Considering the way it is presented to us, there is no doubt that this is a crime driven by property motivation, one that intends to generate an economic benefit to the criminal, since the system user is confronted with an informative message demanding a payment. However, it is not negligible to consider other motivations that may be associated with the attacker’s ego or resentment, competitive effects, or even actions with obfuscated motivations, of political and/or state order.



This is Engineering/Unsplash

Vetores ou metodologias de ataque

A expressão utilizada para nos referirmos à forma como o este tipo de cibercrime ocorre, ou aos métodos utilizados, é o termo “vetor de ataque”.

Os vetores de ataque mais habituais para este tipo de crime, são os seguintes:

- comprometimento de contas internas das instituições, conduzindo os atacantes a obter privilégios de administrador e a instalar o “ransomware” nos sistemas das vítimas. O comprometimento destas contas pode ocorrer através do acesso a bases de passwords previamente obtidas/furtadas de forma ilícita;
- exploração de vulnerabilidades técnicas que possam existir em software usado pelos utilizadores;
- comprometimento através dos sistemas ou formas de acesso remoto às organizações como o RDP (Remote Desktop Protocol), TeamViewer, Anydesk, ...;
- emails fraudulentos - contendo “links” para sites infetados, ficheiros anexados, macros -, geralmente enviados em grandes quantidades (“spam”) ou dirigidos a alvos específicos;
- distribuição do software malicioso em programas de partilha de ficheiros;
- programas que anunciam e fingem ter uma determinada ação, mas que, na realidade, comprometem a segurança do sistema e/ou dos dados do utilizador. É o caso dos anti-vírus falsos, desfragmentadores de disco, e outros;

Como prevenir

- A importância da utilização de múltiplo fator de autenticação em todas as

Do not pay

The decision not to pay the ransom seems obvious to us:

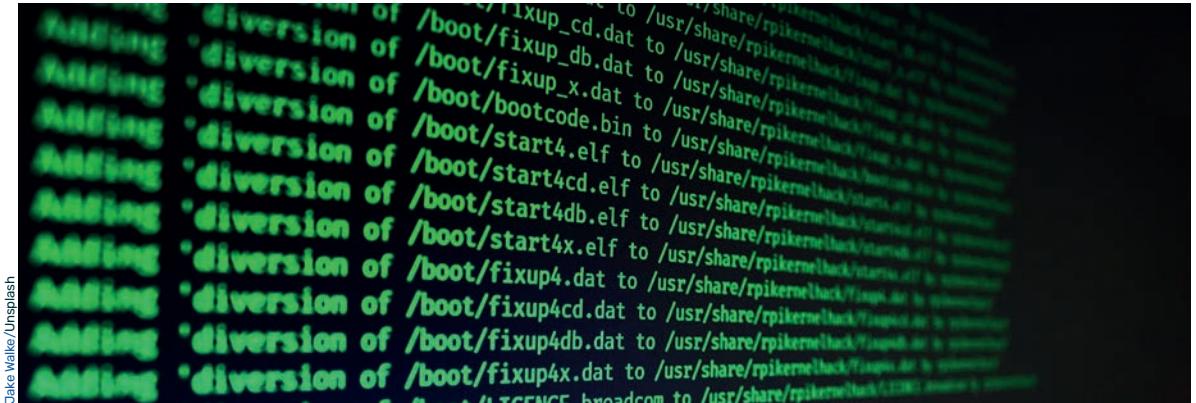
- We will never be sure that the decryption key is obtained;
- The attacker’s logic is to enhance the profit of the criminal activity, expanding the possibility of always extorting more, and increasing the economic gain;
- The *M.O.* is likely to be used and promoted by organised crime, so we cannot guarantee its funding.

Attack vectors or methodologies

The term used to refer to the way this type of cybercrime occurs, or the methods used, is the term ‘attack vector’.

The most common attack vectors for this type of crime are the following:

- Compromising internal accounts of institutions, leading the attackers to gain administrator privileges and install ransomware on the victims’ systems. These accounts can become compromised through access to previously obtained/stolen passwords;
- Exploitation of technical vulnerabilities that may exist in software used by users;
- Compromise through systems or forms of remote access to organisations such as RDP (Remote Desktop Protocol), TeamViewer, Anydesk, ...;
- Fraudulent emails - with links to infected websites, attached files, macros - usually sent in large quantities (spam) or directed to specific targets;
- Distribution of malicious software in file-sharing programs;



contas pessoais e da organização. Este procedimento garante que a haver comprometimento de uma palavra-passe exista um outro fator de identificação e autenticação que limite o acesso ilícito à informação do utilizador;

- sensibilização e atualização de informação sobre as campanhas de phishing, cujos objetivos se centram na captura de acessos de nomes de utilizadores e respetivas palavras-passe;
- realização de exercícios;
- política de armazenamentos (backups) frequentes, com segregação de redes e recurso a dispositivos de memória desconetados da rede. Este cuidado possibilita que os dados cifrados em resultado de um ataque de ransomware, possam efetivamente ser recuperados de um sistema que sabemos não estar infetado;
- manter o software atualizado de modo a instalar eventuais correções de vulnerabilidades técnicas de segurança nos programas utilizados;
- divisão da informação por sub-redes sem interligação, evitando que aquilo que consideramos serem as “jóias da coroa”, ou “informação de valor”, estejam expostas aos atacantes, sem necessidade;

• Programs that advertise and pretend to have a certain action, but that, in reality, compromise the security of the system and/or the user's data. This is the case with fake anti-virus programs, disk defragmenters, and others;

Prevention

- The importance of using multi-factor authentication on all personal and corporate accounts. This procedure ensures that, when a password is compromised, there is another identification and authentication factor that limits illicit access to user information;
- Raising awareness and updating information about phishing campaigns, whose objectives focus on capturing access to user names and passwords;
- Carrying out exercises;
- Having a policy of frequent backups, with segregation of networks and use of memory devices disconnected from the network. This makes it possible for data encrypted following a ransomware attack to be effectively recovered from a system that we know is not infected;
- Keeping the software updated in order to install eventual patches for technical

- abandonar sistemas operativos descontinuados pelo fabricante e substituí-los por outros mais recentes.

Em termos de prioridades, a Polícia Judiciária, através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), considera o combate a este tipo de criminalidade um dos pontos essenciais, quer pelo crescente dano social efetivo quer pelo potencial perigo que previsivelmente crescerá proporcionalmente ao desenvolvimento das tecnologias de informação de uso generalizado.

A atribuição de um crime é sempre importante como instrumento de medida da eficiência do sistema de justiça, sendo nossa preocupação chegar à determinação dos autores destes crimes. No entanto, é igualmente importante a prevenção e a antecipação deste tipo de ataques dirigidos às mais variadas áreas que agora estão suportadas pelas tecnologias de comunicação e informação.

O contexto abriga-nos ainda a perceber, que a investigação destes fenómenos não sobrevive à falta de cooperação, exigindo a todos os atores, nacionais e internacionais, uma partilha célere e efetiva de informação, formação e cultura.

security vulnerabilities in the programs used;

- Dividing the information into subnets without interconnection, preventing what we consider to be the 'crown jewels', or 'valuable information', from being unnecessarily exposed to attackers;

- Abandoning operating systems discontinued by the manufacturer and replacing them with newer ones.

In terms of priorities, the Portuguese Criminal Police, through the National Unit to Combat Cybercrime and Technological Crime (UNC3T), considers combating this type of crime to be one of the key points, both because of the growing effective social damage and the potential danger that is expected to grow proportionally to the development of widely used information technologies.

Attribution of a crime is always important as an instrument to measure the efficiency of the justice system; our concern is to determine the authors of these crimes. However, it is equally important to prevent and anticipate these types of attacks directed at the most diverse areas that are now supported by communication and information technologies.

The context also makes us realise that the investigation of these phenomena does not survive the lack of cooperation, requiring all national and international stakeholders to rapidly and effectively share information, training and culture.



Diários sobre o ransomware LockBit

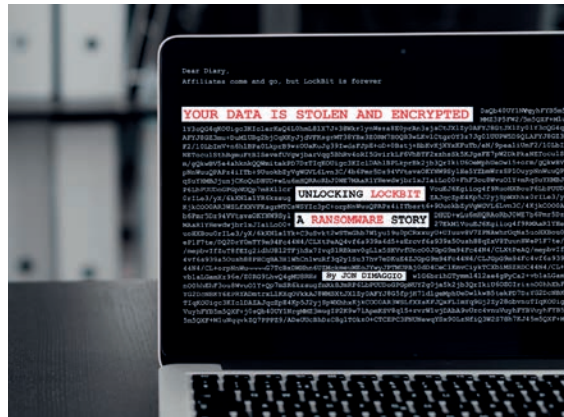
O grupo LockBit, acusado de ataques de ransomware como o recente à empresa [Águas do Porto](#), está ativo e assim vai continuar, apesar dos desaires recentes. Quem o diz é Jon DiMaggio, autor deste documento onde relata como se preparou e acompanhou as atividades do grupo durante mais de dois anos.

“O LockBit não vai desaparecer tão cedo. Apesar da recente negatividade expressa pelos membros da comunidade criminosa, o LockBit gere uma operação lucrativa que é atrativa para os cibercriminosos”, diz. A facilidade na gestão dos ataques de RaaS é uma vantagem, mas o modelo também é suscetível de não ser atualizado ou ser copiado pela concorrência.

A atitude das autoridades perante estes casos deve mudar para “injetar propaganda e desinformação em fóruns escuros da web utilizados pelos criminosos” para “perderem a confiança no fornecedor do RaaS”, porque “paranóia, desconfiança, e preocupações sobre perda de receitas são comuns entre os afiliados do serviço de ransomware”. E o aproveitamento de falhas antigas, a “[maioria](#)” das quais foi usada em ataques durante 2022.

LockBit ransomware diaries

The LockBit group, accused of ransomware attacks such as the one made on the [Águas do Porto](#) company, is active and will remain so, despite the recent setbacks. Who says so is Jon DiMaggio, author of this document where he tells how he prepared and followed the group's activities for more than two years.



‘LockBit is not going away any time soon. Despite the recent negativity expressed by members of the criminal community, LockBit runs a profitable operation that is attractive to cybercriminals,’ he said. The ease of managing RaaS attacks is an advantage,

but the model is also susceptible to not being updated or copied by competitors.

Authorities’ attitude towards these cases must change to ‘inject propaganda and misinformation into dark web forums used by criminals’ in order to ‘lose confidence in the RaaS provider’ as ‘paranoia, mistrust and concerns about lost revenue are common among ransomware service affiliates’. They should also exploit old flaws, the ‘[majority](#)’ of which were used in attacks in 2022.

Estado da legislação sobre o cibercrime

Desde os anos 90 do século passado que vários países começaram a trabalhar em legislação específica para a cibercriminalidade. Atualmente, cerca de 94% dos Estados membros da Organização das Nações Unidas têm legislação nesse sentido.

Nesta atualização do Conselho da Europa, nota-se o problema em muitos países de reformas que “são iniciadas, mas não realizadas, com projetos de lei por vezes pendentes durante anos ou a serem abandonados”, enquanto outros “têm o cuidado de não adotar leis sem as capacidades necessárias para as aplicar”. Também por isso, apenas 43% dos países na ONU são Partes ou Signatários da [Convenção de Budapeste sobre o Cibercrime](#), num total de 83 Estados.

O documento é também relevante para a negociação em curso de uma “Convenção Internacional Abrangente de Combate à Utilização das Tecnologias de Informação e Comunicação para Fins Criminais” das Nações Unidas porque “quanto mais consistente for o texto do futuro tratado com o da Convenção sobre a Cibercriminalidade, tanto mais provável é que se encontre um consenso”.

State of cybercrime legislation

Since the 1990s, several countries began working on legislation specific to cybercrime. Currently, around 94 % of UN member states have legislation dedicated to this area.

In this update by the Council of Europe, one problem seems to be that in many countries, reforms are ‘initiated but not carried through, with draft laws sometimes pending for years or being abandoned’, while others ‘are careful not to adopt laws without the necessary capacities to apply them’. This is also why only 43 % of UN Member States were either Parties or Signatories to the

[Budapest Convention on Cybercrime](#) out of a total of 83 States.

The document is also relevant to the ongoing negotiation of a ‘Comprehensive International

Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes’ by the United Nations because ‘the more consistent the text of the future treaty will be with that of the Convention on Cybercrime, the more likely it is for a consensus to be found’.



LEGISLATION



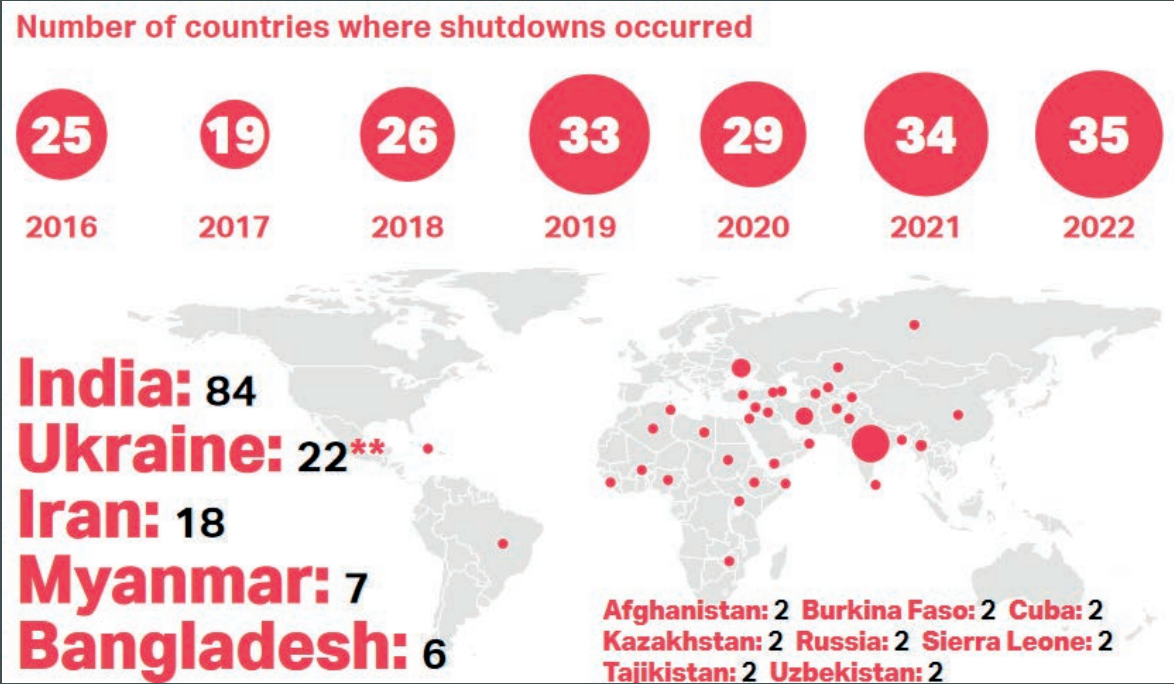
Como a guerra na Ucrânia alterou a paisagem das ciberameaças

[“Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape”](#) é o balanço de um ano de ciberataques após a invasão da Ucrânia pela Rússia. Os ataques a alvos ucranianos aumentaram 250% relativamente a 2020, enquanto os ataques a países da NATO cresceram mais de 300% no mesmo período.

How the Ukraine conflict transformed the cyberthreat landscape

[Fog of War: How the Ukraine Conflict Transformed the Cyber Threat Landscape](#) takes stock of one year of cyberattacks following Russia’s invasion of Ukraine. Attacks on Ukrainian targets increased by 250 % compared to 2020, while attacks on NATO countries grew by more than 300 % in the same period.

 [Weapons of Control, Shields of Impunity: Internet shutdowns in 2022](#)





Diretora | Director

Inês Esteves

Edição | Editor

Pedro Fonseca

Design Gráfico | Graphic Design

Sara Dias

Maria Cristóvão

Tradução | Translation

Sara Pereira

Fotografia (capa e índice) | Photography (cover & index)

This is Engineering/Unsplash

Bence Boros/Unsplash



.....

Publicação trimestral | Quarterly publicatio

Março 2023 | March 2023

