bilingual edition

ptsoc {news}

10

Mês da cibersegurança são todos

3 perguntas a Inês Esteves

O poder da engenharia social: o exemplo do phishing e suas variantes
por Ana Ferreira

Every month is cybersecurity month

3 questions to Inês Esteves

The power of social engineering: the example of phishing and its variants
by Ana Ferreira

.pt

OUTRAS INICIATIVAS

WORKSHOP PTSOC E PSP : DESAFIOS & BOAS PRÁTICAS DE CIBERSEGURANÇA

17 de outubro – Capacitação Digital | Ética e Privacidade, Escola Superior de Tecnologia e Gestão de Leiria

LANÇAMENTO DE 2 MOOCS DE CIBERSEGURANÇA (PLATAFORMA NAU)

30 out - Gestão dos Riscos de Cibersegurança nas Organizações (10h)
30 nov - Gestão da Continuidade de Negócio (10h)

04 **Mês da cibersegurança são todos**
Every month is cybersecurity month

26 **Estatísticas** **Statistics**

O setor da eletricidade está a atrasar-se na cibersegurança? Is the power system lagging behind when it comes to cybersecurity?

Portugal em 32ª na violação de dados pessoais Portugal ranks 32nd in personal data breaches

Custo dos ataques informáticos a longo prazo The long-term cost of cyberattacks

28 **3 perguntas a...**
3 questions to...

Inês Esteves

Membro do Conselho Diretivo do .PT
Member of the Board of Directors of .PT
Head of Cybersecurity

33 **O poder da engenharia social: o exemplo do phishing e suas variantes . The power of social engineering: the example of phishing and its variants**

Ana Ferreira

Cofundadora Women4Cyber Portugal
Co-Founder Women4Cyber Portugal

41 **Documentos** **Documents**

What is Secure? Analysis of Popular Messaging Apps

Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms

Mês da cibersegurança são todos
Every month is cybersecurity month

No Mês Europeu da Cibersegurança, que decorre este outubro, e marcando também a décima edição desta revista publicada pelo PTSOC do .PT, fomos ouvir a opinião de especialistas sobre o exigente momento porque passa a cibersegurança.

Procurou-se ter um conjunto diverso de opiniões (e de factos) que estes responsáveis podem aportar para a atualidade do setor.

Parece existir consenso que a cibercriminalidade está a aumentar, mas é necessário olhar de forma mais refinada para o que nos dizem os números e os intervalos temporais, como o fazem Sónia Martins e Inês Esteves, em 3 Perguntas a…

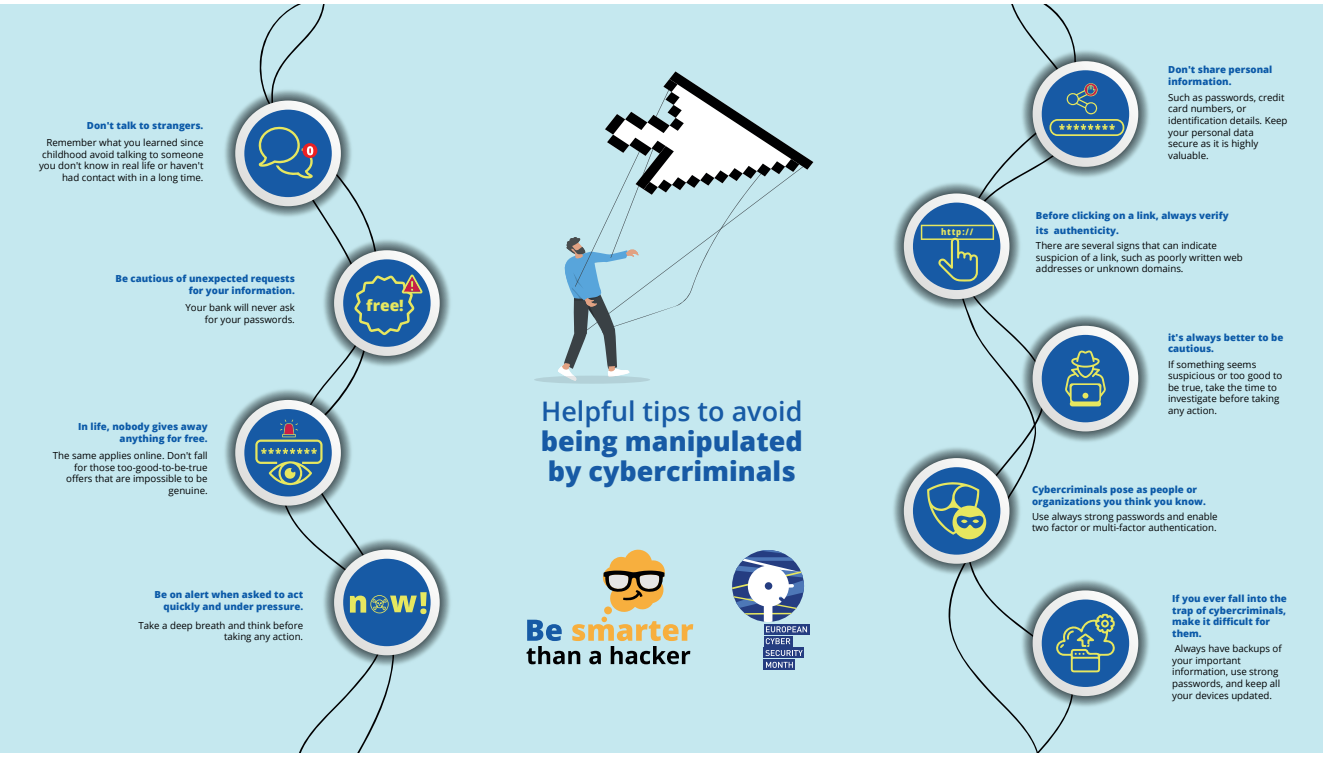
Lino Santos analisa a NIS 2 para Portugal e antecipa que o CNCS está a realizar um relatório para identificação das polí-

During European Cybersecurity Month, which takes place this October, and also marking the 10th edition of this magazine published by .PT PTSOC, we heard the opinions of experts on the challenging times that cybersecurity is going through.

We sought to obtain different opinions (and facts) that these leaders can contribute to the current state of the sector.

There seems to be a consensus that cybercrime is on the rise, but we need to take a more refined look at what the figures and time intervals tell us, as Sónia Martins and Inês Esteves do in 3 Questions to...

Lino Santos takes a look at NIS 2 for Portugal and anticipates that the CNCS is drafting a report to identify



ticas públicas e legislação existente que já respondam aos requisitos da Diretiva.

Marta Moreira Dias desafia as lideranças a assumirem o seu papel imprescindível na cibersegurança, enquanto Miguel Pupo Correia olha para como os riscos podem ser transformados em oportunidades, tanto para organizações como para os cidadãos – uma visão partilhada por Luís Pisco. Na realidade, todos têm de se habituar a ter "hábitos higiénicos", como lhes chama João Damas, para se conseguir ter uma Internet melhor, mais robusta e segura todos os meses e todos os dias.

public policies and existing legislation that already meet the Directive's requirements.

Marta Moreira Dias challenges leaders to take on their indispensable role in cybersecurity, while Miguel Pupo Correia looks at how risks can be transformed into opportunities for both organisations and citizens - a vision shared by Luís Pisco. In reality, everyone has to get used to having 'hygiene habits, as João Damas calls them, in order to achieve a better, more robust and secure Internet every month and every day.

Sónia Martins

Comissário. Chefe do Núcleo de Cibercriminalidade, Departamento de Investigação Criminal da Polícia de Segurança Pública
Commissioner. Head of the Cybercrime Unit, Criminal Investigation Department of the Public Security Police (PSP)

Cibercrimes aumentaram relativamente a 2022. Tendência deve prosseguir em 2024
Cybercrime has increased compared to 2022. Trend to continue in 2024

Neste espaço dedicado à cibersegurança, começo por referir que acreditamos que a mesma constitui uma missão de todos nós, seja no desempenho do papel de funcionários de uma instituição do setor público ou privado, seja enquanto especialistas com responsabilidade nesta matéria, seja enquanto utilizadores individuais de plataformas, de aplicações e de serviços online.

Cada um de nós, no seu nível de ação potencial, deve efetuar uma utilização consciente e responsável das capacidades que o ciberespaço e a tecnologia colocam à sua disposição e desempenhar um papel ativo na cibersegurança relativa a si próprio e na que respeita à sua própria organização.

O Núcleo de Cibercriminalidade da Polícia de Segurança Pública (NCIBER/PSP), que completa três anos em novembro, foi criado com um propósito muito bem definido e com vista a suprir uma necessidade decorrente das transformações que se vêm operando nos tipos de crime com que a PSP lida mais

In this space dedicated to cybersecurity, I'll start by saying that we believe it is a mission for all of us, whether as employees of a public or private sector institution, as specialists with responsibility in this area or as individual users of online platforms, applications and services.

Each of us, at our potential level of action, must make a conscious and responsible use of what cyberspace and technology make available to us and play an active role in cybersecurity for ourselves and for our own organisation.

The Public Security Police Cybercrime Centre (NCIBER/PSP), which turns three in November, was created with a very well-defined purpose in mind and with a view to meeting a need arising from the changes that have been taking place in the types of crime that PSP deals with most closely - which are also those that most directly affect citizens. As a result, the NCIBER was strategically created to support PSP's

proximamente e que também são aqueles que mais diretamente afetam os cidadãos. Por conseguinte, o NCIBER foi criado estrategicamente com o intuito de apoiar investigações da PSP a nível nacional, em que o recurso ao ciberespaço e aos meios informáticos e tecnológicos têm um carácter instrumental para a prática de crimes.

Estamos a referir-nos aos crimes ditos "tradicionais", que sempre existiram e que já eram (também) da competência de investigação da PSP, mas que agora verificamos que os autores recorrem a novos meios e a um novo espaço para o seu cometimento, e/ou aqueles cuja competência de investigação seja delegada pelo Ministério Público na PSP.

Da análise que podemos efetuar, até à data, a PSP, no ano de 2023, deparou-se com um aumento de casos de burlas informáticas e nas comunicações, comparativamente com igual período de 2022.

Dos fenómenos que a PSP acompanha, destacamos a tendência crescente dos últimos anos relativamente a situações de utilização de plataformas online e criação de 'sites' falsos para fins de cometimento de burlas relacionadas com a compra e venda de viaturas (cujos números até agosto de 2023 já ultrapassaram os totais de 2022), falsos arrendamentos e a compra e venda de artigos diversos.

Na sequência do acompanhamento de dados do RASI, em 2023, a PSP continua a registar

nation-wide investigations in which the use of cyberspace and computer and technological means are instrumental to the commission of crimes.

We are referring to the so-called 'traditional' crimes, which have always existed and which were (also) already under PSP's investigative competence, but which we now see their perpetrators using new means and a new space to commit them, and/or those whose investigative competence is delegated by the Public Prosecution Service to PSP.

From the analysis we can make, to date, in 2023 PSP has seen an increase in cases of computer and communications fraud, compared to the same period in 2022.

Of the phenomena that PSP is monitoring, we would highlight the growing trend in recent years regarding situations involving the use of online platforms and the creation of fake websites for the purpose of committing scams related to the purchase and sale of vehicles (the numbers of which up to August 2023 have already exceeded the totals for 2022), fake leases and the purchase and sale of miscellaneous items.

Following the monitoring of RASI data in 2023, PSP continues to record a significant number of reports of fraud associated with the use of the MBWay app. The phenomenon that stands out the most refers to incidents classified as fraud - false family member,

várias denúncias, em número significativo, de burla associada à utilização da aplicação MBWay, sendo que o fenómeno que mais se destaca são as ocorrências enquadráveis no crime de burla – falso familiar, designado "Olá Pai Olá Mãe". Para a prática deste crime, os suspeitos, através de mensagem escrita em aplicação de comunicação (maioritariamente WhatsApp), apresentam-se como um familiar muito próximo (filh@) da potencial vítima. Não obstante os vários alertas que já foram realizados sobre este tipo de burla, os números, até agosto de 2023, já duplicaram os totais de 2022.

Os factos acima descritos são uma preocupação para a PSP, a par de todas as outras tipologias criminais que investiga e procura prevenir e mitigar. Por este motivo e devido às características transnacionais do próprio cibercrime, tem existido uma forte aposta da PSP na cooperação policial nacional e internacional, no estabelecimento de protocolos com outras entidades de outros setores, bem como na participação em projetos de prevenção da cibercriminalidade nacionais e internacionais, destacando a colaboração da PSP com a .PT nos Workshops de Cibersegurança, no âmbito do Programa Roteiro INCoDe.2030 e a participação conjunta da PSP e da PJ, enquanto representação portuguesa em projetos internacionais, onde diversos países desenvolvem ações conjuntas e massivas de prevenção da cibercriminalidade, dirigidas aos jovens.

Foto de ROBIN WORRALL - Unsplash

known as 'Hi Mum Hi Dad'. In order to commit this crime, the suspects pose as a close relative (a child) of the potential victim via a written message on a communication application (mostly WhatsApp). Despite the various warnings that have already been issued about this type of scam, the figures up to August 2023 have already doubled the totals for 2022.

The above described facts are a concern for PSP, along with all the other types of crime it investigates and seeks to prevent and mitigate. For this reason, and due to the transnational characteristics of cybercrime itself, PSP has made a strong commitment to national and international police cooperation, establishing protocols with other entities from other sectors and participating in national and international cybercrime prevention projects. Noteworthy is PSP's collaboration with .PT in the Cybersecurity Workshops under the INCoDe.2030 Roadmap Programme and the joint participation of PSP and PJ as Portuguese representatives

Mais recentemente, numa destas iniciativas, foi igualmente possível contar com a colaboração do CNCS. Acreditamos que o futuro passa também por esta forma de colaboração, multissetorial, multidimensional e multipolicial. O próprio cibercrime, em muitas das suas facetas, faz-se valer de uma conjugação de esforços de diversas valências, de diferentes cibercriminosos, para a concretização dos seus fins.

Relativamente a 2024, parece-nos verosímil que as tendências observadas pela PSP em 2023 se mantenham.

Também acreditamos que a engenharia social e, em particular, o phishing (incluindo as suas variantes smishing e vishing), continuem a ser amplamente utilizados pelos cibercriminosos, uma vez que constituem técnicas que recorrem ao engano para manipular a perceção das pessoas, levando-as a divulgarem informações confidenciais ou pessoais, que podem ser utilizadas para fins fraudulentos.

Por fim, realça-se o surgimento de novos perigos e ameaças decorrentes do recurso à Inteligência Artificial para a criação de código de malware e de phishing, criação de e-mails, mensagens e sites altamente credíveis, com vista a enganar as vítimas e levá-las a partilhar dados sensíveis, para além da facilitação da tradução de textos ("translation as a crime").

in international projects where various countries are carrying out massive joint cybercrime prevention initiatives aimed at young people.

More recently, in one of these initiatives, it was also possible to count with CNCS' collaboration. We believe that the future also lies in this form of multisectoral, multidimensional and multipolicy collaboration. In order to achieve its ends, in many of its facets, cybercrime itself makes use of a combination of efforts from different areas and different cybercriminals.

With regard to 2024, it seems likely that the trends observed by PSP in 2023 will continue.

We also believe that social engineering, namely phishing (including its smishing and vishing variants), will continue to be widely used by cybercriminals, as these are techniques that use deception to manipulate people's perceptions, leading them to disclose confidential or personal information that can be used for fraudulent purposes.

Finally, we would like to highlight the new dangers and threats arising from the use of Artificial Intelligence to create malware and phishing code, the creation of highly credible emails, messages and websites to trick victims into sharing sensitive data, as well as the facilitation of text translation ('translation as a crime').

Por todos estes motivos, reforçamos uma vez mais o papel ativo que cada um deve ter na sua própria cibersegurança, sendo que a defesa contra as diferentes formas de cibercriminalidade é tão forte quanto o elo mais fraco, que continua a ser o fator humano.

For all these reasons, we once again reinforce the active role that each of us must play in our own cybersecurity, since the defence against the different forms of cybercrime is only as strong as its weakest link, which continues to be the human factor.

Marta Moreira Dias

Membro do Conselho Diretivo do .PT | Head of Legal & Corporate Affairs
.PT Board of directors | | Head of Legal & Corporate Affairs

Casa roubada, trancas à porta
Shut the stable door after the horse has bolted

Casa roubada, trancas à porta. A sabedoria popular ajuda-nos. Não conseguiria legendar melhor o retrato da cibersegurança no espaço temporal 2022-2023. A perceção e a identificação do problema foram feitas de forma massiva e estenderam-se a todas as geografias.

Hoje, ninguém acredita que esta regra tenha exceções. Pessoas, empresas, organizações e Estados foram vítimas e, também por isso, obrigados a reagir ou, pelo menos, a ficar alerta. O legislador europeu não hesitou e construiu um quadro legal que, sendo desafiante para qualquer intérprete do direito, tem bases sólidas e profundamente enraizadas em princípios de colaboração e reciprocidade.

Shut the stable door after the horse has bolted. Popular wisdom can help us. I could not have painted a better picture of cybersecurity in the 2022-2023 timeframe. The problem was perceived and identified on a massive scale and spread to all geographies.

Nowadays, nobody believes that this rule has any exceptions. People, companies, organisations and states have all been victims and are therefore forced to react or at least be alert. The European legislator did not hesitate to create a legal framework that, while challenging for any interpreter of the law, has solid foundations and is deeply rooted in principles of collaboration and

Não poderá ser outra a abordagem quando falamos de problemas transnacionais.

Em momento anterior, tivemos oportunidade de nos debruçar sobre o quadro normativo, maioritariamente de fonte comunitária, que hoje regula a cibersegurança a nível nacional e de enfatizar o problema da diversidade regulatória, sobretudo no espaço europeu, notadamente ao nível da concorrência entre os players do mercado dos 27, mas, talvez mais preocupante, fora fronteiras da União Europeia (UE) onde o chamado "Brussels Effect" pode ser altamente condicionante. Em suma, se no âmbito da proteção jurídica falarmos aqui de metas - seja em 2023, seja para o futuro próximo -, idealmente todos devemos trabalhar na prevenção do cibercrime e na mitigação e tratamento da cibersegurança. Prevenir e reagir. Parece fácil, mas não é. Os desafios são muitos, e elencaremos apenas alguns.

Pessoas, empresas, organizações e Estados foram vítimas e, também por isso, obrigados a reagir ou, pelo menos, a ficar alerta.

Desde a (boa) transposição de instrumentos legislativos como a Diretiva NIS2, passando pela criação de mecanismos de enforcement e, no caso concreto de empresas e organizações, de regras claras de compliance e, fundamental, de capacitação de pessoas e estruturas organizacionais, no sentido não só da formação e sensibilização, mas também alocação das adequadas, seguras e sustentáveis infraestruturas digitais de su-

reciprocity. The approach cannot be any different when it comes to transnational problems.

Earlier, we had the opportunity to look at the regulatory framework, mostly from EU sources, that currently regulates cybersecurity at national level. We were able to emphasise the problem of regulatory diversity, especially in the European area, notably in terms of competition between the EU-27 players in the market, but perhaps more worryingly, outside the European Union (EU) borders where the so-called 'Brussels Effect' can be highly conditioning. In short, if we are talking about legal protection goals - in 2023 or in the near future - ideally we should all work on preventing cybercrime and mitigating and dealing with cybersecurity. Prevent and react. It sounds easy, but it isn't. The challenges are many, and we will list just a few.

People, companies, organisations and states have all been victims and are therefore forced to react or at least be alert.

From the (good) transposition of legislative instruments such as the NIS2 Directive to the creation of enforcement mechanisms and, in the specific case of companies and organisations, clear compliance rules and, fundamentally, the empowerment of people and organisational structures, not only in terms of training and awareness, but also considering the allocation of adequate,

porte. A receita parece óbvia, agora, para ser executada precisamos de recursos financeiros robustos e de uma efetiva cultura interna de cibersegurança. A implementação do RGPD começou a trilhar este caminho, que sem dúvida agora se afigura bem mais tortuoso. Mas caminharemos em conjunto e a importância desta opção está espelhada em iniciativas nacionais recentes e naquilo que são as opções do legislador, matéria que me é especialmente cara.

Senão vejamos: no passado mês de maio, via D.L n.º 34/2023, foi formalmente criada a Cyber Academia and Innovation Hub, com uma missão muito clara e alinhada com a Estratégia Nacional de Ciberdefesa e com a Estratégia Nacional de Segurança do Ciberespaço 2019-2023, de promover e realizar atividades de interesse público nas áreas da cibersegurança e da ciberdefesa.

Um dos propósitos desta associação é promover a capacitação dos recursos humanos afetos à ciberdefesa e à cibersegurança. Considerando que no leque de fundadores temos, entre outros, o Centro Nacional de Cibersegurança e a Polícia Judiciária, não podemos deixar de ter elevadas expetativas, nobres objetivos conduzidos por quem de direito.

Os estatutos desta Associação abrem a possibilidade de adesão de novos associados, facto que nos parece fazer todo o sentido e que esperamos venha a ser uma realidade.

secure and sustainable digital support infrastructures. The recipe seems obvious, but in order to implement it we need robust financial resources and an effective internal cybersecurity culture. The implementation of the GDPR has started us down this path, which undoubtedly now seems much more tortuous. But we will move forward together. The importance of this choice is reflected in recent Portuguese initiatives and in the legislator's choices, a subject that is particularly close to my heart.

Let's take a look: last May, via Decree-Law 34/2023, the Cyber Academia and Innovation Hub was formally created, with a very clear mission in line with the National Cyberdefence Strategy and the National Strategy for Cyberspace Security 2019-2023, to promote and carry out activities of public interest in the areas of cybersecurity and cyberdefence.

One of this association's aims is to promote the training of human resources involved in cyberdefence and cybersecurity. Considering that its founding members include the Portuguese National Cybersecurity Centre and Polícia Judiciária [Portuguese Criminal Police], we can't help but have high expectations, and noble objectives led by those in the know.

The Association's statutes open up the possibility of new members joining, which seems to make perfect sense to us and

Neste mesmo âmbito da colaboração, noutra oportunidade demos nota que a própria NIS2 veio incentivar os Estados-Membros à criação de parcerias público-privadas para fins de troca de conhecimentos, alertas, exercícios em matéria de ciberameaças e partilha de boas práticas. Mas não ficamos por aqui: o legislador comunitário está apostado em criar um terreno fértil para a mobilização institucional e multissetorial, inclusive além-fronteiras.

Na primeira semana de abril foi publicado, para efeitos de consulta pública, o Cyber Solidarity Act (Lei da Solidariedade Cibernética, em tradução livre) que, na sua essência, pretende impulsionar a cooperação a nível da UE na preparação e resposta a grandes ciberataques. O Regulamento prevê, a mero título de exemplo, o estabelecimento do designado Escudo Cibernético Europeu, composto por Centros de Operações de Segurança (SOC) nacionais e transfronteiriços.

Relembramos aqui que o .PT gere o seu próprio PTSOC desde 2020, com resultados muito interessantes ao nível da deteção, resposta e prevenção de incidentes e ameaças de cibersegurança na zona pt. Facto que, *per si*, revela a relevância desta tipologia de serviços nas organizações.

which we hope will become a reality.

In the same context of collaboration, on another occasion we noted that the NIS2 itself encouraged member states to create public-private partnerships to exchange knowledge, alerts, cyberthreat exercises and share their best practices. But that's not all: the EU legislator is committed to creating fertile ground for institutional and multisectoral mobilisation, including across borders.

In the first week of April, the Cyber Solidarity Act was published for public consultation. It essentially aims to boost cooperation at EU level in preparing for and responding to major cyberattacks. As an example, the Regulation provides for the establishment of the so-called European Cyber Shield, made up of Portuguese and cross-border Security Operations Centres (SOC).

Let us remember that .PT has been running its own PTSOC since 2020, with very interesting results in terms of detecting, responding to and preventing cybersecurity incidents and threats in the .pt zone. This, in itself, shows how important this typology of service is for organisations.

Aprender e não errar de novo, será o propósito do estabelecimento de um mecanismo de revisão de incidentes de segurança cibernética, também tipificado neste diploma, que irá rever e analisar os principais incidentes após a sua ocorrência para, assim, enformar os desenvolvimentos futuros da abordagem europeia à segurança cibernética.

Esta visão holística do tema da cibersegurança dá-nos, enquanto cidadãos, algumas garantias para o futuro. Mas as trancas da porta não podem constituir-se como espartilhos à eficiência, à agilidade e à inovação. Fica o desafio para as lideranças.

Learning and not making mistakes again will be the purpose of establishing a cybersecurity incident review mechanism, also typified in this law, which will review and analyse the main incidents after they have occurred in order to shape future developments in the European approach to cybersecurity.

This holistic view of cybersecurity gives us, as citizens, some guarantees for the future. But putting a lock on the stable door cannot be a barrier to efficiency, agility and innovation. Leaders are still faced with challenges.

Lino Santos

Coordenador do Centro Nacional de CIbersegurança
Coordinator of the National Cybersecurity Centre

Impacto e futuro da Diretiva NIS 2 em Portugal
Impact and future of the NIS 2 Directive in Portugal

Dia 16 de janeiro deste ano entrou em vigor a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União. Também conhecida como NIS 2, esta Diretiva visa o robustecimento

On 16 January 2023, Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union came into force. Also known as NIS 2, this Directive aims to strengthen the resilience of

da resiliência das redes e dos sistemas de informação que suportam os serviços considerados essenciais – e agora também os considerados importantes – para a nossa sociedade, incluindo um significativo alargamento do número de setores abrangidos.

O seu texto traz um conjunto de novidades das quais destaco aqui algumas.

No tocante à estrutura e quadro da cibersegurança, esta nova Diretiva vem reforçar as competências da Rede europeia de equipas de reação a ciberincidentes (EU CSIRT Network) e do grupo de cooperação, e formalizar uma rede de organizações de coordenação de cibercrises (UE-CyCLONe) que articulará, quando necessário, com mecanismo integrado da UE de resposta política a situações de crise (mecanismo IPCR). Para este efeito, Portugal precisa de identificar uma autoridade de gestão de crises e incidentes de cibersegurança de grande escala que reúna, debaixo de uma unidade de coordenação, o conjunto das autoridades nacionais com responsabilidades operacionais no ciberespaço.

A NIS 2 vem igualmente influenciar uma nova Estratégia Nacional de Segurança do Ciberespaço, atualmente em fase de elaboração no seio do Conselho Superior de Segurança do Ciberespaço. Neste contexto, os Estados-membros são chamados a definir políticas de ciberproteção ativa, focadas na prevenção, deteção, monitorização, análise

networks and information systems that support services deemed essential - and now also those considered important - for our society, including a significant extension of the number of sectors covered.

Its wording contains several new features, some of which I would like to highlight here.

With regard to the structure and framework of cybersecurity, this new Directive reinforces the competences of the European Network of Cyber Security Incident Response Team (EU CSIRT Network) and the cooperation group, and formalises a cyber crisis liaison organisation network (EU-CyCLONe) that will coordinate, when necessary, with the EU's integrated political crisis response mechanism (IPCR mechanism). In order for

e atenuação de violações da segurança das redes, de uma forma ativa, combinadas com a utilização de capacidades internas e externas à rede da vítima.

Esta visão, mais pró-ativa e menos reativa, reforça o papel do PANORAMA e a sua integração numa futura rede europeia de SOCs, como instrumento de fusão e de produção de informação acionável para o ciberespaço nacional, e em particular para os operadores de serviços essenciais, operadores de infraestruturas críticas e principais organismos da Administração Pública.

Por outro lado, a NIS 2 insta os Estados-membros a criar um quadro para divulgação coordenada de vulnerabilidades.

A divulgação coordenada de vulnerabilidades especifica um processo estruturado e mediado pelo CSIRT nacional, mediante o qual as vulnerabilidades são notificadas aos fabricantes ou fornecedores de produtos de TIC ou aos prestadores de serviços de TIC potencialmente vulneráveis de uma forma que lhes permite diagnosticar e corrigir as vulnera-

this to happen, Portugal must identify a large-scale cybersecurity incident and crisis management authority that brings together, under one coordination unit, all the national authorities with operational responsibilities in cyberspace.

The NIS 2 also influences a new National Strategy for Cyberspace Security, currently under development by the High Council for Cyberspace Security. In this context, member states are asked to define active cyber protection policies, focused on actively preventing, detecting, monitoring, analysing and mitigating network security breaches, combined with the use of internal and external capabilities to the victim's network.

This vision, more proactive and less reactive, reinforces the role of PANORAMA and its integration into a future European network of SOCs as an instrument for merging and producing actionable information for the national cyberspace, namely for operators of essential services, operators of critical infrastructures and key public administration bodies.

bilidades antes de serem divulgadas informações pormenorizadas sobre as mesmas a terceiros ou ao público.

Para a melhor eficácia de um instrumento desta natureza, é da maior importância a criação de mecanismos de comunicação anónima de vulnerabilidades, bem como de um quadro de proteção para os peritos que investigam estas vulnerabilidades, nomeadamente quanto à sua potencial sujeição à responsabilidade penal.

Por último, esta é uma importante oportunidade para desenvolver e melhorar a atual estrutura e o quadro da cibersegurança nacional, aproveitando a transposição desta Diretiva para corrigir aspetos menos conseguidos e incorporar algumas lições aprendidas no decurso dos últimos anos. Refiro-me, por exemplo, a uma melhor definição do âmbito subjetivo de aplicação, a uma clarificação das obrigações para as entidades reguladas, assegurando uma adequação dessas obrigações à criticidade e risco das entidades e dos serviços que prestam à sociedade, a uma melhor eficácia dos instrumentos de resposta a incidentes, bem como ao reforço do Quadro Nacional de Referência para a Cibersegurança e dos seus instrumentos acessórios neste contexto.

Tendo em vista a sua transposição, o Centro Nacional de Cibersegurança, no âmbito do Observatório de Cibersegurança, encontra-se a realizar um relatório sobre o impacto

On the other hand, the NIS 2 urges member states to create a framework for coordinated vulnerability disclosure.

Coordinated vulnerability disclosure specifies a structured process, mediated by the national CSIRT, whereby vulnerabilities are notified to potentially vulnerable ICT product manufacturers/suppliers or to ICT service providers so they can diagnose and fix the vulnerabilities detected before detailed information about them is disclosed to third parties or to the public. For such an instrument to be effective, it is of the utmost importance to create mechanisms for anonymised reporting of vulnerabilities, as well as a framework of protection for the experts investigating these vulnerabilities, namely regarding their potential criminal liability.

Finally, this is an important opportunity to develop and improve the current structure and framework of national cybersecurity, taking advantage of the transposition of this Directive to correct less successful aspects and incorporate some lessons learnt over the last few years. I am referring, for example, to a better definition of the subjective scope of application, a clarification of the obligations or regulated entities, ensuring these obligations are appropriate to the criticality and risk of the entities and the services they provide to society, a better effectiveness of incident response tools, as well as the strengthening of the National Cybersecurity

em Portugal da Diretiva NIS 2 prevendo a identificação das políticas públicas e legislação atualmente existentes que já respondam aos requisitos da NIS 2;

• A identificação das alterações preconizadas pela NIS 2 em relação à NIS 1, no que respeita à Lei n.º 46/2018, de 13 de agosto, que estabelece o regime jurídico da segurança do ciberespaço e respetivos diplomas complementares, incluindo a apresentação de propostas de alteração legislativa;

• A identificação das alterações preconizadas pela NIS 2 em relação à NIS 1, com implicações noutros diplomas legais, incluindo a apresentação de propostas de alteração legislativa; bem como a avaliação de impacto para o exercício das competências das autoridades competentes em cibersegurança e a sua relação com autoridades competentes setoriais.

Com este relatório pretende-se apoiar o poder político na formulação de uma proposta de Lei que altera o atual Regime Jurídico de Segurança do Ciberespaço.

Framework and its ancillary tools in this context.

With a view to its transposition, the Portuguese National Cybersecurity Centre, as part of the Cybersecurity Observatory, is preparing a report on the impact of the NIS 2 Directive in Portugal, identifying the already existing public policies and legislation that already meet the NIS 2 requirements:

• Identifying the changes recommended by the NIS 2 in relation to the NIS 1, with regard to Law 46/2018 of 13 August, which establishes the legal framework for cyberspace security and its complementary legislation, including the presentation of proposals for legislative amendments;

• Impact and future of the NIS 2 Directive in Portugal Identifying the changes recommended by the NIS 2 in relation to the NIS 1, with implications for other laws, including the presentation of proposals for legislative amendments, as well as the impact assessment for the exercise of the competences of the competent authorities in cybersecurity and their relationship with sectoral competent authorities.

This report aims to support the political authorities when it comes to formulating a proposal for a Law amending the current Legal Framework for Cyberspace Security.

Miguel Pupo Correia

Professor Catedrático, Instituto Superior Técnico/INESC-ID,
Membro não executivo do Conselho Diretivo do .PT
Full Professor, Instituto Superior Técnico/INESC-ID
Non-executive member of .PT Board of Directors

Cibersegurança: do risco à oportunidade
Cybersecurity: from risk to opportunity

Há quem pense que a cibersegurança diz respeito à proteção integral de sistemas tecnológicos e organizações face a ataques realizados por via informática e pela Internet. No entanto, é fácil compreender que essa proteção integral é tão realista quanto a possibilidade de reduzir a zero o crime numa grande cidade: não é realista.

Assim sendo, a cibersegurança tem que ver com gestão de risco. O objetivo da cibersegurança não é reduzir o risco a zero, mas mantê-lo num nível suficientemente baixo. O risco depende de três fatores: nível de ameaça, nível de vulnerabilidade e impacto de um ataque bem sucedido. Às organizações cabe sobretudo atuar na redução do seu nível de vulnerabilidade, de modo a reduzirem o risco ao tal nível suficientemente baixo.

Quanto mais não fosse, as notícias que aparecem na comunicação social bastariam para mostrar que esse simples objetivo de manter baixo o nível de vulnerabilidade é

Some people think that cybersecurity refers to the comprehensive protection of technological systems and organisations against attacks carried out via computers and the Internet. However, it is easy to realise that such comprehensive protection is about as realistic as the possibility of reducing crime to zero in a large city: not realistic at all.

Cybersecurity is about risk management. The aim of cybersecurity is not to reduce risk to zero, but to keep it at a sufficiently low level. Risk depends on three factors: the level of threat, the level of vulnerability and the impact of a successful attack. It is, above all, up to organisations to act to reduce their level of vulnerability in order to reduce the risk to a sufficiently low level.

If nothing else, the news in the media would be enough to show how this simple objective of keeping the level of vulnerability low is anything but simple. What this article aims

tudo menos simples. O ponto deste artigo é: não será que um nível baixo de vulnerabilidade – a cibersegurança – não será também uma oportunidade?

A Distributed Ledger Technology (DLT), muitas vezes designada tecnologia Blockchain, mostra isso mesmo: que uma infraestrutura altamente segura é uma oportunidade para a criação de novas aplicações informáticas que podem transformar o mundo. A primeira Blockchain era uma componente do sistema informático que implementava uma criptomoeda chamada Bitcoin. O uso dessa infraestrutura altamente segura permitiu que essa criptomoeda hoje esteja valorizada em 500 mil milhões de euros. Ou seja, um mero conjunto de computadores interligados de

at is this: isn't a low level of vulnerability - cybersecurity - also an opportunity?

Distributed Ledger Technology (DLT), often referred to as Blockchain technology, shows just that: that a highly secure infrastructure is an opportunity to create new IT applications that can transform the world. The first Blockchain was a computer system component that implemented a cryptocurrency called Bitcoin. The use of this highly secure infrastructure has allowed this cryptocurrency to be valued today at 500 billion euros. In other words, a simple set of computers interconnected to provide a highly secure application can be worth a fortune.

Foto de Pierre Borthiry - Peiobty, Unsplash

forma a fornecerem uma aplicação altamente segura consegue valer uma fortuna.

A DLT, incluindo a Blockchain da Bitcoin, consegue um nível muito elevado de cibersegurança (ou um nível de vulnerabilidade muito baixo) usando uma solução técnica designada replicação. Apesar de os detalhes serem complicados, a ideia é simples: todos os dados de transações (transferências de valor) estão copiados num número elevado de computadores (milhares de computadores, no caso da Bitcoin). Assim, é possível confiar nessa informação sem confiar nos, ou sequer conhecer os, donos desses computadores. Não se pode confiar em cada um, mas pode-se confiar no sistema como um todo. Confia-se ao nível de 500 mil milhões de euros.

A Bitcoin foi apenas o princípio. Estas infraestruturas são agora a base de uma nova visão designada Web 3. As aplicações serão já não criptomoedas, mas várias aplicações de finanças distribuídas, de gestão de identidade de pessoas e organizações, de documento certificados, de venda de bens móveis e imóveis, etc.

Assim, a cibersegurança deixa de ser apenas a solução para um risco, passando a ser uma oportunidade para a criação de uma nova economia e de um novo ecossistema que permitirá facilitar a nossa vida de cidadãos e das organizações.

DLT, including the Bitcoin Blockchain, achieves a very high level of cybersecurity (or a very low level of vulnerability) using a technical solution called 'replication'. Although details are complex, the idea is simple: all transaction data (transfers of value) is copied onto a large number of computers (thousands of computers, in the case of Bitcoin). Like so, it is possible to trust this information without trusting, or even knowing, the owners of these computers. You can't trust each one, but you can trust the system as a whole. And your trust can be worth 500 billion euros.

Bitcoin was just the beginning. These infrastructures are now the basis of a new vision known as Web 3. The applications will no longer be cryptocurrencies, but various distributed finance applications, identity management for people and organisations, certified documents, the sale of movable and immovable property, etc.

In this way, cybersecurity is no longer just a solution to a risk, but rather an opportunity to create a new economy and a new ecosystem that will make life easier for us as citizens and organisations.

Luis Pisco

Departamento Jurídico e Económico da DECO
DECO's Legal and Economic Department

A cibersegurança e o comportamento dos consumidores
Cybersecurity and consumer behaviour

Durante a pandemia que assolou a vida de todos, confinando-nos ao espaço dos nossos lares e tendo como contacto privilegiado com o mundo exterior a internet, habituámo-nos a utilizar o ambiente online como uma extensão das nossas vidas, seja para lazer, trabalhar ou fazer compras. Pode-se afirmar que houve um "boom" na utilização do ambiente digital para realizar uma parte significativa das nossas atividades. E essa maior utilização dos benefícios da internet veio para ficar, mesmo depois da pandemia ter acabado.

Infelizmente, assistimos também a um violento aumento de ciberataques a consumidores, empresas e organizações das áreas mais diversas, desde a saúde, media ou mesmo operadores de comunicações eletrónicas, expondo as muitas fragilidades de empresas e organizações em matéria de cibersegurança.

Ora, o aumento de ocorrência destes ataques aumentou igualmente o sentimento de insegurança e a própria confiança dos consumidores clientes/utilizadores dos serviços online dessas organizações, potenciando

During the pandemic that has devastated everyone's lives, locking us in our homes and having the Internet as our privileged contact with the outside world, we have become accustomed to using the online environment as an extension of our lives, be it for leisure, work or shopping. It could be said that there has been a boom in the use of the digital environment to carry out a significant part of our activities. And even after the pandemic is over, this increased use of the Internet's benefits is here to stay.

Unfortunately, we have also seen a violent increase in cyberattacks on consumers, companies and organisations in the most diverse areas, from health to the media and even electronic communications operators, exposing companies and organisations' many weaknesses when it comes to cybersecurity.

However, the increased occurrence of these attacks has also increased the feeling of insecurity and the very confidence of consumers who are customers/users of

um impacto naturalmente negativo no seu comportamento, na forma como passam a utilizar, ou não, esses serviços no futuro. Essa desconfiança afasta os consumidores.

De facto, a perceção dos consumidores sobre os efeitos de um ciberataque, com a potencial violação dos seus dados pessoais, privacidade e exposição a fraudes, abala naturalmente a sua confiança nas organizações e marcas atacadas, sendo um fator suscetível de, por si só, poder vir a alterar os comportamentos e hábitos de consumo relacionados com as mesmas.

Na verdade, o furto de dados pessoais de clientes a uma empresa pode acabar por resultar numa multiplicidade de ataques individuais aos mesmos, gerando uma massificação de ataques com efeitos extremamente nocivos para as vítimas, como furtos de identidade, fraude com cartões bancários ou golpes de engenharia social.

Daí a cada vez maior importância de uma aposta decidida e robusta na cibersegurança por parte das organizações, enquanto fator gerador de confiança entre os clientes e até uma vantagem competitiva perante concorrentes, gerando um valor reputacional inestimável, particularmente se essa postura passar ainda pelo investimento em ações informativas e de literacia digital junto dos utilizadores dos seus serviços digitais, ensinando-os a navegar seguros online.

these organisations' online services, which naturally has a negative impact on their behaviour and on how they will or will not use these services in the future. This distrust alienates consumers.

In fact, consumers' perception of the effects of a cyberattack, with the potential violation of their personal data, privacy and exposure to fraud, naturally undermines their trust in the organisations and brands under attack, and is a factor that could, in itself, change consumers behaviour and consumption habits towards them.

As a matter of fact, the theft of customers' personal data from a company can end up resulting in several individual attacks on them, generating mass attacks with extremely damaging effects for the victims, such as identity theft, bank card fraud or social engineering scams.

This is why it is increasingly important for organisations to make a decisive and robust commitment to cybersecurity, as a trust-generating factor for customers. It can even be seen as a competitive advantage over competitors, generating invaluable reputational value, especially if organisations also invest in informative and digital literacy initiatives for users of its digital services, teaching them how to navigate safely online.

João Damas

Investigador sénior, APNIC Labs; Consultor do .PT
Senior Researcher, APNIC Labs; .PT Consultant

KINDNS, a gentileza no DNS
KINDNS, kindness at DNS

A Internet (com I maiúsculo) é, como o nome indica, uma rede de redes inter-conectadas, cada uma a funcionar de forma autónoma mas utilizando uma série de protocolos comuns que fazem possível a interconexão. Talvez paradoxalmente o TCP/IP, apesar do nome, não é necessariamente um deles. Os verdadeiramente indispensáveis são os protocolos que permitem a dispositivos em redes diferentes saber como estabelecer ligações entre eles. Na Internet existem dois destes protocolos: o BGP, o protocolo de routing entre redes independentes, e o DNS, quando usa o nome do espaço de nomes único da Internet.

Vista a operação autónoma de cada rede, às vezes dão-se situações para tratar de melhorar o comportamento do sistema de routing da Internet.

Há alguns anos, a Internet Society (ISOC) começou um programa que estabelecia uma série de "normas de comportamento" de adoção voluntária em cada rede e que contribuiriam para uma melhora do funcionamento da rede e evitar alguns problemas de segurança na rede. O programa chama-se Mutually Agreed Norms for Routing Security (MANRS), um jogo com a palavra inglesa manners, referente a boa educação entre pessoas.

Mais recentemente, a ICANN, vistos alguns pro-

The Internet (with a capital I) is, as the name suggests, a network of interconnected networks, each operating autonomously via a series of common protocols that enable interconnection. Perhaps paradoxically, the TCP/IP is not, despite its name, necessarily one of them. Really indispensable are the protocols that allow devices on different networks to know how to establish connections between them. There are two such protocols on the Internet: BGP, the routing protocol between independent networks, and DNS, which uses the name of the Internet's unique namespace.

Given the autonomous operation of each network, situations sometimes arise to try to improve the behaviour of the Internet routing system.

A few years ago, the Internet Society (ISOC) started a programme to establish 'behaviour norms' that could be adopted voluntarily by each network in order to help improve the functioning of the network and avoid certain network security problems. The programme is called Mutually Agreed Norms for Routing Security (MANRS), a play on the word manners.

More recently, ICANN, seeing some similar problems in the DNS and Internet naming space,

blemas parecidos no espaço do DNS e os nomes de Internet, arrancou um programa chamado Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS), fazendo também um jogo de palavras com o inglês *kindness*.

É que uma parte fundamental da segurança e fortaleza da Internet depende dos hábitos higiénicos que todos os operadores tenham nas suas formas habituais de implementar e operar a sua rede.

O programa KINDNS oferece informação e dicas para cada tipo de operador do DNS, desde os provedores de DNS autoritativo a qualquer nível até aos operadores de DNS recursivos (normalmente provedores de Internet ou companhias com redes próprias de qualquer tamanho).

Junto com as recomendações, que vão acompanhadas de alguns tutoriais para diferentes plataformas e que vão incorporando novos materiais de forma continuada, está disponível também, um self-test que indica o nível de concordância entre os nossos serviços e as recomendações com vista a avaliar que modificações seriam necessárias para melhor aderir a esta estrutura de gentileza e boa educação para os nossos clientes e o resto da Internet.

Como no caso do MANRS, o mais provável é que o nível de participação cresça lentamente no início para depois aumentar de ritmo e passar a ser visto como uma marca de serviço de qualidade. Entretanto, se ter um bom serviço é um dos nossos objetivos, aderir a estes "hábitos higiénicos" pode ser vantajoso.

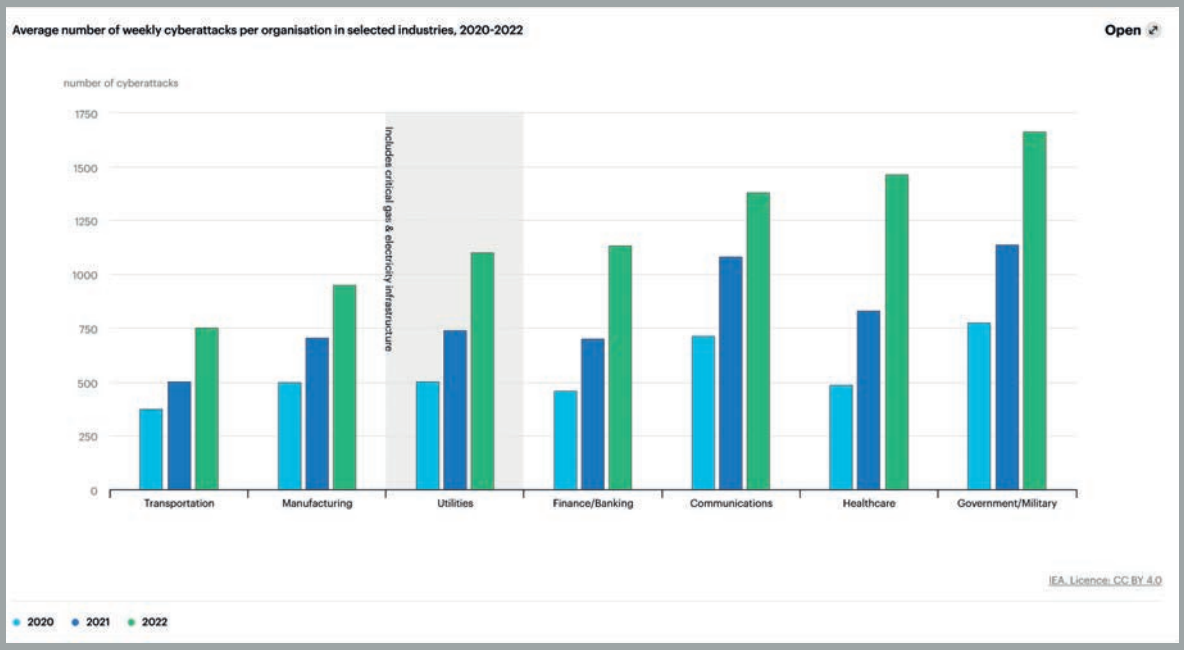
launched a programme called Knowledge-Sharing and Instantiating Norms for DNS and Naming Security (KINDNS), also a play on the word kindness.

A fundamental part of the security and strength of the Internet depends on the hygiene habits that all operators have in their usual ways of implementing and operating their network.

The KINDNS programme offers information and tips for every type of DNS operator, from authoritative DNS providers at any level to recursive DNS operators (usually Internet providers or companies with their own networks of any size).

Along with the recommendations, which also include tutorials for different platforms and which incorporate new material on an ongoing basis, there is also a self-test that indicates the level of agreement between our services and the recommendations; it assesses what changes would be necessary to better adhere to this framework of kindness and good manners for our customers and the rest of the Internet.

As with MANRS, the level of participation will most likely grow slowly at first and then pick up pace and come to be seen as a staple of quality service. However, if having a good service is one of our goals, adhering to these 'hygiene habits' can be advantageous.



O setor da eletricidade está a atrasar-se na cibersegurança?

Os ciberataques estão a aumentar no setor elétrico. Estes serviços "enfrentam sérias dificuldades em encontrar e manter profissionais qualificados necessários para se defenderem", constata a Agência Internacional da Energia (IEA).

Os sistemas digitais, equipamentos de telecomunicações e sensores na rede aumentam a exposição, "uma vez que cada elemento constitui um ponto de entrada adicional para as organizações cibercriminosas". Por exemplo, ciberataques recentes no setor "desativaram controlos remotos dos parques eólicos, interromperam contadores pré-pagos (...) e conduziram a violações de dados recorrentes envolvendo" informação sensível dos clientes.

Is the power system lagging behind when it comes to cybersecurity?

Cyberattacks are on the rise in the electricity sector. These utilities 'face serious difficulties in finding and retaining the skilled professionals needed to defend themselves,' notes the International Energy Agency (IEA).

Digital systems, telecommunications equipment and sensors throughout the grid increase their exposure, 'as each element provides an additional entry point for cybercriminal organisations.' For example, recent cyberattacks in the sector 'have disabled remote controls for wind farms, disrupted prepaid meters (...) and led to recurrent data breaches involving" client sensible information.

Portugal em 32ª na violação de dados pessoais

Na "classificação" mundial de contas pessoais acedidas ilegalmente, Portugal ocupa o 32º lugar. Entre 2004 e a atualidade, foram acedidas quase 48 milhões de contas, de um total global de 16.482 milhões.

A TAP lidera os acessos indevidos, com 1.2 milhões em agosto de 2022, seguindo-se o site de conteúdos gerados por utilizador Wattpad (em junho de 2020, com quase 700 mil registos) e o serviço de avatares online Gravatar em outubro desse ano, com 388 mil dados pessoais violados.

Portugal ranks 32nd in personal data breaches

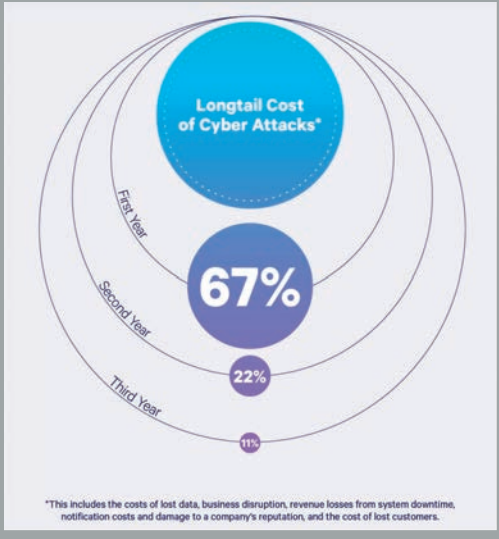
In the global ranking of illegally accessed personal accounts, Portugal ranks 32nd. Between 2004 and today, almost 48 million accounts have been accessed, out of a global total of 16 482 million.

Portuguese airline TAP Air Portugal leads the way in data breaches, with 1.2 million in August 2022, followed by Wattpad, the user-generated content website (in June 2020, with almost 700 000 records) and the online avatar service Gravatar in October 2020, with 388 000 personal data breaches.

Custo dos ataques informáticos a longo prazo

Os custos a curto prazo (três anos) de uma violação de dados podem prolongar-se por meses ou anos e incluem despesas que as empresas não conhecem ou não antecipam.

Nestes custos incluem-se perda de dados, disrupção do negócio, perdas de receitas pela inatividade do sistema, custos de notificação ou danos reputacionais da marca.



The long-term cost of cyberattacks

The short-term costs (three years) of a data breach can extend over months or even years and include expenses that companies are not aware of or do not anticipate.

These costs include loss of data, business disruption, loss of revenue due to system downtime, notification costs or reputational damage to the brand.

3

Inês Esteves

Membro do Conselho Diretivo do .PT
Head of Cyber Security
Member of the Board of Directors of .PT
Head of Cybersecurity

1. Como se pode avaliar o setor da cibersegurança este ano?

No rescaldo de 2022, um ano negro para a cibersegurança, que ficou marcado não só pelo aumento sem precedentes de ciberataques, mas também pela complexidade e maior sofisticação dos meios utilizados para comprometer severamente as operações de vários setores críticos, que alcançaram grande exposição mediática e resultaram em elevados danos financeiros e reputacionais como os perpetrados contra a imprensa, telecomunicações, energia, saúde, defesa e transportes, 2023 trouxe uma maior perceção do risco de sofrer um ataque de cibersegurança e maior consciência que estamos todos (empresas, organizações e cidadãos) vulneráveis a ataques, uma consciência de que urge concretizar em qualificações e competências em matéria de cibersegurança.

Ainda que em termos globais as ciberameaças tenham aumentado no primeiro semestre de 2023, assistimos (por ora) a uma

1. How can we assess the cybersecurity sector's performance for this year?

In the aftermath of 2022, a dark year for cybersecurity, marked not only by the unprecedented increase in cyberattacks, but also by the complexity and greater sophistication of the means used to severely compromise the operations of several critical sectors, which achieved great media exposure and resulted in high financial and reputational damages such as those perpetrated against the press, telecommunications, energy, health, defence and transport, 2023 brought a greater perception of the risk of suffering a cybersecurity attack and greater awareness that we are all (companies, organisations and citizens) vulnerable to attacks, an awareness that needs to be implemented in cybersecurity qualifications and skills.

Although in global terms cyberthreats increased in the first half of 2023, we are witnessing (for now) a slowdown in the growth of incidents recorded in Portugal, compared to the same period last year, with phishing/smishing/vishing (to which we dedicate special reference in this editions' tutorial), ransomware (see 'Ransomware, a "pure computer crime", in PTSOC {news} #8), online scams and social engineering lead the list of incidents. This is also the trend we observe at the .PT Security Operations Centre (PTSOC): a less pronounced growth

desaceleração do crescimento do número de incidentes registados no contexto nacional, em comparação com o período homólogo, com o phishing/smishing/vishing (a que dedicamos especial referência no nosso tutorial desta edição), ransomware (ver "Ransomware, um 'crime informático puro'", na PTSOC {news} #8), as burlas online e a engenharia social a liderar a lista de incidentes. Esta é também a tendência que observamos no Centro de Operações de Segurança do .PT (PTSOC): um crescimento menos acentuado do número de incidentes reportados nos nossos canais públicos e privados de comunicação.

Mas não nos enganemos, esta desaceleração não é um ponto de inflexão da tendência de crescimento do cibercrime verificada nos últimos anos, amplificada pelo contexto de pandemia Covid-19 e agravada pela situação de guerra na Europa. Como, aliás, antecipa o Relatório de Riscos Globais de 2023 do World Economic Forum, que identifica a generalização do cibercrime e a insegurança cibernética entre os 10 principais riscos mundiais no período de 2 a 10 anos.

2. Quais as tendências e principais vetores de ataques que se podem antecipar para 2024?

O mundo está e será cada vez mais digital, tecnológico e interconectado, o que traz enormes oportunidades, mas também uma maior exposição das organizações, empresas

in the incidents reported on our public and private communication channels.

But let us not be mistaken, this slowdown is not an inflection point in the growth trend of cybercrime seen in recent years, amplified by the context of the COVID-19 pandemic and aggravated by the war in Europe - as the 2023 Global Risks Report of the World Economic Forum anticipates, which identifies the generalisation of cybercrime and cyber insecurity among the 10 main global risks in the period of 2 to 10 years.

2. What are the trends and main attack vectors that can be anticipated for 2024?

The world is and will be increasingly digital, technological and interconnected. With it, come enormous opportunities, but also a greater exposure of organisations, companies and citizens to the risks and threats of cyberspace. Given that, we inevitably anticipate an increase in the number and impact of security incidents, namely through the growth and professionalisation of cybercriminal groups dedicated to Ransomware-as-a-Service (RaaS), which offer third parties platforms and complete services that allow for the perpetration and dissemination of this type of attack, without the need for technical knowledge. Another trend to follow is the increasingly sophisticated Spear Phishing. Focused on specific targets, it uses carefully crafted

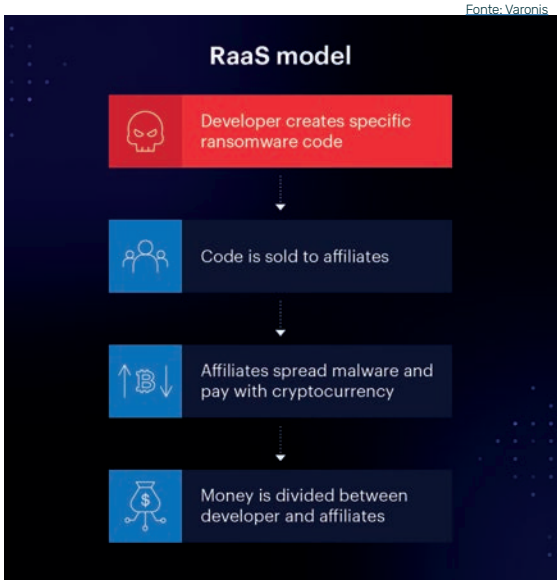
e cidadãos aos riscos e ameaças do ciberespaço. Neste contexto, antecipa-se, inevitavelmente, o aumento do número e impacto dos incidentes de segurança, em especial, através do crescimento e profissionalização de grupos cibercriminosos dedicados ao Ransomware-as-a-Service (RaaS), que oferecem a terceiros plataformas e serviços completos que permitem perpetrar e massificar esta tipologia de ataques, sem que seja necessário conhecimento técnico. Também o Spear Phishing, cada vez mais sofisticado, que visa alvos específicos com mensagens personalizadas, cuidadosamente elaboradas utilizando informação de fontes públicas, que tornam estas mensagens praticamente indistinguíveis de comunicações legítimas, é uma tendência a acompanhar.

Estas técnicas serão amplificadas através do recurso a Inteligência Artificial (IA) e "machine learning" (ML) que permitem analisar e processar grandes volumes de dados, em tempo real, automatizar e introduzir elevados níveis de sofisticação nesta tipologia de ataques.

A crescente importância do uso da Cloud traz também consigo complexas considerações de cibersegurança inerentes ao armazenamento de dados e aplicativos fora da esfera física e geográfica das organizações e, muitas vezes, em vários ambientes. Não obstante a maior maturidade e robustez das atuais capacidades da Cloud, o crescimento dos dados e a evolução das necessidades

personalised messages with information from public sources, which makes these messages practically indistinguishable from legitimate communications.

Fonte: Varonis



These techniques will be amplified through the use of Artificial Intelligence (AI) and machine learning (ML) that make it possible to analyse and process large volumes of data, in real time, automating and introducing high levels of sophistication in this type of attacks.

The growing importance of using Cloud services also brings with it complex cybersecurity considerations inherent to storing data and apps outside the physical and geographic sphere of organisations themselves, often in multiple environments. Despite the greater maturity and robustness

de negócio estão a expandir a superfície de ataques.

Nota ainda para o crescimento de ciberameaças resultantes da maior conectividade 5G em conjugação com a maior adoção de dispositivos IoT, nomeadamente através do crescimento em frequência e volumetria dos ataques de negação de serviço distribuídos (DDoS).

Longe de uma visão pessimista da evolução do ciberespaço e da tecnologia, com certeza do seu enorme potencial enquanto motor de inovação, inclusão, modernização, desenvolvimento económico e social, a compreensão das ameaças e a exposição aos riscos é o ponto de partida para preparar e trabalhar na sua prevenção.

3. Qual deve ser o posicionamento das organizações em 2024?

Se nos últimos anos as empresas e organizações estiveram focadas na transição para o digital redefinindo as suas estratégias e processos de negócio, adaptando a tecnologia à rápida e massiva evolução operada, é tempo e reveste urgência autonomizar a cibersegurança da gestão habitual das equipas de TI e incorporá-la como prioridade do negócio e dos líderes. Os níveis de maturidade de cibersegurança das organizações dependem mais da maturidade dos seus líderes do que da dimensão e da

of current Cloud capabilities, data growth and evolving business needs are expanding the attack surface.

Note also the growth of cyberthreats resulting from greater 5G connectivity, together with the increased use of IoT devices, namely through the growth in frequency and volume of distributed denial of service (DDoS) attacks.

Far from a pessimistic view of the evolution of cyberspace and technology, certainly of its enormous potential as a driver of innovation, inclusion, modernisation, economic and social development, understanding threats and exposure to risks is the starting point to prepare and work on its prevention.

3. What should organisations be doing in 2024?

If, in recent years, companies and organisations have been focused on the transition to digital, redefining their strategies and business processes, adapting technology to the rapid and massive evolution that is taking place, it is time and urgent to make cybersecurity autonomous from the usual management of IT teams and incorporate it as a priority for businesses and leaders. The cybersecurity maturity levels of organisations depend more on the maturity of their leaders than on the size and financial investment capacity

capacidade financeira de investimento das organizações.

Sendo certo que não existe uma arquitetura ou fórmula que possa garantir segurança absoluta contra ciberataques, identificam-se cinco áreas de atuação que devem ser endereçadas na estratégia de segurança das organizações:

•envolvimento transversal e liderança nos temas da cibersegurança, posicionando-se como uma prioridade na estratégia de transformação digital;

•planeamento e processos robustos, em particular, na definição de planos de resposta e recuperação de incidentes;

•metodologias de identificação e gestão de riscos (incluindo a cadeia logística) e plano de continuidade de negócio;

•aposta clara na capacitação e literacia em cibersegurança, através da formação e desenvolvimento de novas competências enquanto vetor estratégico para a proteção da organização;

• foco na cooperação e na responsabilidade partilhada nos temas da cibersegurança, identificando e estabelecendo parcerias sólidas que permitirão a resposta mais eficaz a ameaças e riscos cibernéticos cada vez mais complexos, contribuindo para construção de ecossistema mais forte e resiliente.

of the organisations themselves.

While it is true that there is no architecture or formula that can guarantee absolute security against cyberattacks, five areas of action are identified that must be addressed in organisations' security strategy:

•Transversal involvement and leadership in cybersecurity issues, positioning itself as a priority in the digital transformation strategy;

•Robust planning and processes, namely in the definition of incident response and recovery plans;

•Risk identification and management methodologies (including the logistics chain) and business continuity plan;

•Clear commitment to empowerment and literacy in cybersecurity, through the training and development of new skills as a strategic vector for protecting the organisation;

•Focus on cooperation and shared responsibility in cybersecurity issues, identifying and establishing solid partnerships that will enable a more effective response to increasingly complex cyberthreats and risks, contributing to building a stronger and more resilient ecosystem.

Ana Ferreira

Cofundadora da Women4Cyber Portugal
Co-Founder Women4Cyber Portugal

O poder da engenharia social: o exemplo do phishing e suas variantes

No contexto da cibersegurança, a engenharia social consiste na utilização de técnicas para influenciar e manipular indivíduos a revelarem informação pessoal ou sensível, ou executarem determinada ação que não é legítima, ou que os pode prejudicar, por exemplo, financeiramente.

Phishing

O phishing pertence à família de ataques de engenharia social cujo principal objetivo é obter credenciais de acesso a contas de email ou contas bancárias online, dados de cartões de crédito ou outro tipo de informação pessoal ou sensível. Se estes ataques forem bem-sucedidos podem abrir portas para que, ataques mais sofisticados e com maior impacto e gravidade, possam ser executados. Exemplos disso são: o roubo financeiro, o roubo de identidade, a extorsão, o bloqueio no acesso aos dados ou a impossibilidade de executar transações bancárias.

Métodos de *phishing*

Na base de um ataque de phishing está normalmente um email com características aparentemente legítimas, com o intuito de pedir que o utilizador execute determinada ação, cujo resultado será ir para uma página para pedir dados extra, no que parece ser uma ação rotineira e le-

The power of social engineering: the example of phishing and its variants

In cybersecurity, social engineering consists of using techniques to influence and manipulate individuals into revealing personal or sensitive information, or performing a certain action deemed illegitimate or that could harm them financially, for example.

Phishing

Phishing belongs to the family of social engineering attacks whose main aim is to obtain access credentials to email or online bank accounts, credit card details or other types of personal or sensitive information. Should these attacks be successful, they can open the door to more sophisticated ones with a greater impact and severity. Examples of phishing include financial theft, identity theft, extortion, blocking data access or the impossibility of carrying out banking transactions.

Phishing methods

Most phishing attacks usually start with an apparently legitimate email, with the intention of asking the user to perform a given action, following which the user will access a secondary page asking for additional data, in

gítima. Um dos primeiros ataques de phishing, de onde o próprio nome derivou, foi executado em 1996, quando criminosos se fizeram passar por membros do staff da empresa America Online (AOL), com o objetivo de pedir às potenciais vítimas as credenciais de acesso às suas contas. A razão deste pedido prendia-se com a necessidade de verificar e corrigir informação de pagamentos ou dados das próprias contas.

Um outro ataque de phishing foi novamente massificado em 2003, quando criminosos começaram a criar mensagens de email bastante convincentes, manipulando as suas vítimas a clicar num link para poderem efetuar a atualização das suas contas bancárias. Os criminosos usariam depois o acesso às contas das vítimas para efetuar atos ilegais, como compras não autorizadas ou roubo financeiro.

Desde então, estes ataques têm aumentado de forma exponencial e têm vindo a explorar novos contextos como a indicação de que a vítima ganhou ou pode ganhar valores avultados de dinheiro. Este tipo de ataques pode mesmo incluir a necessidade da vítima ligar para um número telefónico, onde uma gravação pede para indicar o seu número de cartão de crédito ou do cartão de cidadão, para se poder autenticar e usufruir do benefício indicado. Atualmente, os criminosos mascaram-se atrás de grandes empresas e bancos mundialmente conhecidos como o Loyds Bank, o HSBC, a Amazon ou o Paypal, mas podem também usar empresas ou instituições que tenham alguma relação com as vítimas (como DHL, FedEx ou CTT).

what appears to be a routine and legitimate action. One of the first phishing attacks, from which the name itself derives, was carried out in 1996, when criminals posed as America Online (AOL) staff, with the aim of asking potential victims for their account access credentials. This request was being made in order to verify and correct payment information or account data.

Another phishing attack was again widespread in 2003, when criminals began creating very convincing email messages, manipulating their victims into clicking on a link in order to update their bank accounts. The criminals would then use access to the victims' accounts to carry out illegal acts, such as unauthorised purchases or financial theft.

Since then, these attacks have increased exponentially and have been exploring new contexts such as informing the victim they have won or could win large amounts of money. This type of attack may even include the need for the victim to call a given telephone number, where a recording asks them to provide their credit card or identity card number, in order to authenticate themselves and enjoy the aforementioned benefit. Criminals are currently masking themselves behind large companies and world-renowned banks such as Lloyds Bank, HSBC, Amazon or PayPal, but they can also use companies or institutions that have some relationship with

Para além de mensagens de email, os criminosos podem criar websites muito semelhantes aos legítimos para onde atraem as vítimas a partir de mensagens de email ou de outros websites, convidando-as a fornecer dados pessoais ou informação sensível que podem posteriormente explorar em seu benefício, como por exemplo, para preencher os dados do seu cartão matriz. Neste caso, existe mesmo a possibilidade de usarem endereços Web (URLs) que incluem praticamente o mesmo domínio que os endereços legítimos. Por exemplo, no caso da Amazon, o seu site original (www.amazon.com) poderia ser alterado para www.amazaon.com, ou outra combinação do género. Para os mais atentos, isto pode não ser o suficiente para serem enganados, mas é possível executar um programa na página Web em questão (usando JavaScript), que coloca visível o endereço legítimo, mas este mascara o incorreto na hora de submeter a informação pedida.

Outro exemplo é o aparecimento de janelas pop-up que pedem à vítima informação pessoal ou sensível, enquanto esta navega no sítio original. Isto pode não levantar suspeitas já que não há alteração de endereço ou da página original, na interação com essas janelas.

Phishing personalizado: o *spear-phishing*

Emails de phishing com conteúdos genéricos são bastante fáceis de criar e partilhar a grande velocidade na Internet. Mesmo que haja apenas uma pequena percentagem de vítimas a serem exploradas, já vale a pena o lucro obtido, dada a simplicidade do ataque. No entanto, quando a

the victims (such as DHL, FedEx or CTT).

In addition to email messages, criminals can create websites very similar to the legitimate ones where they lure victims through email messages or other websites, inviting them to provide personal data or sensitive information that they can later exploit for their benefit, for example, to fill in the data on your matrix card. In this case, there is even the possibility of using web addresses (URLs) that include practically the same domain as those of legitimate addresses. For example, with Amazon, its original website (www.amazon.com) could be changed to www.amazaon.com, or to another similar combination. For those with an attentive eye, this may not be enough to deceive them, but it is possible to run a program on the web page in question (using JavaScript), which makes the legitimate address visible, but masks the incorrect one when submitting the requested information.

Another example are pop-up windows that ask the victim for personal or sensitive information while they are browsing the original website. This may not arouse suspicion since there is no change of address or original page when interacting with these windows.

Personalised phishing: spear-phishing

Phishing emails with generic content are fairly easy to create and share at high speed on the Internet. Even if only a small

necessidade de sucesso por parte de um atacante é maior, o foco é geralmente direcionado para um alvo específico como, por exemplo, um administrador de redes ou de sistemas. Desta forma, o conteúdo do email necessita de ser adaptado às preferências, hábitos de utilização ou outras características do destinatário, podendo isto exigir mais recursos por parte dos criminosos. No entanto, este processo vai garantir uma maior probabilidade de sucesso na hora de convencer as potenciais vítimas que a sua história é legítima.

Este tipo de phishing é designado de spear-phishing porque, tal como uma lança, o alvo a atingir está bem definido. Se este alvo se focar essencialmente em indivíduos em cargos executivos ou em cargos de grande responsabilidade numa organização, que têm obviamente muitos privilégios e poder de decisão, então este ataque ganha um novo nome: whaling spear phishing ("caça à baleia").

Smishing

Muitas vezes, o ataque adequa-se e replica-se em tecnologias ou dispositivos diferentes, como é o caso do smishing. Neste ataque de phishing, em vez do email ou de sítios Web, os criminosos enviam mensagens via SMS (Short Message Service) para convencer as vítimas a fornecerem dados pessoais ou privados. Estas mensagens podem também conter links para sítios maliciosos.

percentage of victims are exploited, it is worth the profit, given the simplicity of the attack. However, when an attacker has a greater need for success, the focus is usually on a specific target, such as a network or system administrator. For this goal, the email needs to be adapted to the preferences, usage habits or other characteristics of the recipient, which may require more resources on the criminals' part. However, this process will guarantee a greater chance of success when it comes to convincing potential victims that their story is legitimate.

This type of phishing is called 'spear-phishing' because, like a spear, the target is well defined. If this target is essentially comprised of individuals in executive positions or positions of great responsibility within an organisation, who obviously have a lot of privilege and decision-making power, then this attack takes on a new name: 'whaling spear phishing'.

Smishing

The attack is often adapted and replicated on different technologies or devices, as is the case with smishing. With this phishing attack, instead of resorting to emails or websites, criminals send txt messages to persuade victims to share personal or private data. These messages can also contain links to malicious websites.

Vishing

Outro tipo de phishing, o vishing (ou VoIP phishing, de Voice over Internet Protocol), utiliza chamadas de voz para iludir ou manipular as vítimas a fornecer informação pessoal ou sensível a entidades não autorizadas, tal como nos ataques anteriores. Neste caso, os criminosos podem efetuar chamadas de voz ou deixar mensagens gravadas. Este contacto telefónico pode ainda ser precedido por mensagens de texto, para maior probabilidade de sucesso.

Pharming

Este é um ataque que corrompe o DNS (Domain Name Server – Nome do Servidor do Domínio), de uma rede para que os endereços de sítios legítimos cujas vítimas pedem acesso, sejam resolvidos ou traduzidos em endereços de servidores não autorizados. A alteração não autorizada do DNS é designada de DNS Poisoning. Ao efetuar este "envenenamento" dos mecanismos de resolução de nome, será possível manipular as páginas que serão mostradas às vítimas do ataque de pharming.

Malware

Para além do roubo de dados pessoais ou sensíveis, os ataques de phishing podem abrir portas para que código malicioso (malware: vírus, worms, ransomware, cavalos de tróia, etc.) possa ser executado do lado das vítimas e causar danos, quer no equipamento das mesmas, quer propagar-se a toda a rede onde o equipamento esteja ligado.

Vishing

Another type of phishing is 'vishing' (or 'VoIP phishing', which stands for 'Voice over Internet Protocol'), uses voice calls to trick or manipulate victims into providing personal or sensitive information to unauthorised entities, as in the previous attacks. In this case, criminals can make voice telephone calls or leave recorded messages. This telephone contact can also be preceded by text messages, for a greater chance of success.

Pharming

This is an attack that corrupts a network's DNS (Domain Name Server) so that addresses of legitimate websites whose victims are requesting access to are resolved or translated into the addresses of unauthorised servers. Unauthorised alteration of the DNS is known as 'DNS Poisoning'. By 'poisoning' the name resolution mechanisms, it is possible to manipulate the pages that will be shown to pharming attack victims.

Malware

In addition to stealing personal or sensitive data, phishing attacks can open the door for malicious code (malware: viruses, worms, ransomware, Trojans, etc.) to be executed on the victim's side and cause damage, either to their equipment or spreading to the entire network where the equipment is connected to.

Como Prevenir

Visto serem, na sua maioria, ataques individualizados que chegam a cada caixa de email separadamente, os ataques de phishing são dos mais difíceis de prevenir, porque está nas mãos de cada indivíduo que recebe estas mensagens ter a atenção e o discernimento adequados para poder identificar e mitigar o risco. Adicionalmente, existe a necessidade de reportar esta situação aos demais colegas, familiares ou outros, para que estes sejam alertados e evitem situações perigosas.

Existem, no entanto, algumas boas práticas, que devem ser sempre consideradas para ajudar na prevenção e mitigação de ataques de phishing, quer a nível individual, quer a nível empresarial ou institucional:

Duvidar de emails que pedem para alterar dados de contas ou avisos que estas vão ser bloqueadas, se não agir rapidamente (princípio de persuasão de urgência que motiva os indivíduos a agir rapidamente sem grande análise dos riscos envolvidos);

Verificar sempre junto da empresa ou indivíduo que supostamente enviou a mensagem se esta é legítima;

Verificar sempre a autenticidade do endereço do sítio antes de clicar em qualquer endereço Web ou fornecer informação confidencial por este meio;

Prevention techniques

Since these are mostly individualised attacks that reach each email box separately, phishing attacks are one of the most difficult ones to prevent, as it is up to each individual who receives these messages to given them the appropriate attention and have the discernment to be able to identify and mitigate the risk. In addition, there is a need to report this situation to other colleagues, family members or others, so that they can be alerted and avoid dangerous situations.

There are, however, some good practices that should always be considered to help prevent and mitigate phishing attacks, both at an individual level and at a corporate/institutional level:

Be wary of emails asking you to change your account details or warning you that your account will be blocked if you don't act quickly (the persuasive principle of urgency, which motivates people to act quickly without analysing the risks involved);

Always check with the company or individual who supposedly sent the message that it is a legitimate one;

Always check the authenticity of the website address before clicking on any web address or providing confidential information by this means;

Verificar se o endereço da página Web tem erros ou palavras menos comuns;

Não clicar no link do email, mas se for mesmo necessário, preencher manualmente o endereço do link diretamente na página Web;

Dados mais sensíveis ou pessoais só devem ser comunicados usando o protocolo TLS (verifique se o endereço Web contém HTTPS e verifique também se o certificado é válido clicando no aloquete fechado);

Nunca partilhar informação pessoal ou confidencial por email;

Nunca partilhar informação pessoal ou confidencial por telefone, a não ser que tenha a certeza da autenticidade da pessoa com quem está a falar;

Manter sempre o software, programas de anti-vírus e de anti-malware atualizados;

Implementar autenticação de múltiplo fator sempre que possível, em especial, no acesso a contas com requisitos de proteção extra, como por exemplo, com elevados privilégios de acesso;

Reforçar a educação e atenção junto dos colaboradores, familiares e amigos.

Check the webpages address for errors or less common words;

Do not click on the link in the email; if necessary, manually type the link address directly on the webpage;

More sensitive or personal data should only be communicated using the TLS protocol (check that the web address contains HTTPS and check that the certificate is valid by clicking on the closed lock);

Never share personal or confidential information by email;

Never share personal or confidential information by telephone, unless you are sure of the authenticity of the person you are talking to;

Always keep software, anti-virus and anti-malware programmes up to date;

Whenever possible, implement multi-factor authentication, especially when accessing accounts with extra protection requirements, such as high access privileges;

Reinforce education and attention among employees, family and friends.

O *phishing* veio para ficar

A atenção a ataques de phishing tem de ser constante. Estes vão-se tornar cada vez mais sofisticados e massificados com a utilização de tecnologias como a Inteligência Artificial (IA) e motores que facilmente conseguem identificar o perfil de interação ou a pegada digital de cada utilizador. Com a IA será muito mais fácil e rápido criar conteúdos não só de texto, mas até de voz e imagem falsos, e será muito difícil refutar a sua legitimidade e autenticidade.

Apesar de tudo isto, temos de evidenciar e promover as nossas características de atenção, análise de risco e desconfiança, tal como o fazemos no mundo mais "físico". A falta de tempo, distração, muitas tarefas a executar e a automatização de hábitos inconscientes que bloqueiam a análise consciente do que se passa à nossa volta, não podem ser mais as desculpas usadas.

O bom senso, espírito crítico e a análise de risco, enfim, características humanas de discernimento e decisão, têm de estar alerta a todo o momento.

Phishing is here to stay

Attention to phishing attacks must be constant. These will become increasingly sophisticated and widespread with the use of technologies such as Artificial Intelligence (AI) and engines that can easily identify each user's interaction profile or digital footprint. With AI, it will be much easier and quicker to create fake content, not just text, but even voice and image contents, and it will be very difficult to disprove its legitimacy and authenticity.

Despite all this, we have to emphasise and promote our attentiveness, risk analysis and distrust, just as we do in the more 'physical' world. Lack of time, distraction, too many tasks to do and the automatisation of unconscious habits that block us from consciously analysing what's going on around us can no longer be excuses.

Common sense, critical thinking and risk analysis, in short, human characteristics of discernment and decision-making, must be alert at all times.

What is Secure? Analysis of Popular Messaging Apps

Entre Setembro de 2022 e Maio passado, a Tech Policy Press analisou as aplicações de mensagens Apple Messages, Messages (Google), Messenger da Meta, Signal, Telegram e WhatsApp. O resultado mostra como "os utilizadores estão muitas vezes a voar às cegas. Mesmo os mais preocupados com a privacidade raramente têm informações suficientes para tomar decisões que sejam do seu próprio interesse", no uso destas aplicações. A Signal é elogiada como "a única" que tem medidas para esconder alguns dados dos utilizadores.

Between September 2022 and last May, Tech Policy Press analysed Apple Messages, Messages (Google), Meta's Messenger, Signal, Telegram and WhatsApp messaging apps. The result shows how 'users are too often flying blind. Even those most concerned about privacy rarely have sufficient information to make decisions that are in their own best interest' when using these apps. Signal is praised as 'the only app' that has taken steps to hide some users' data.

Toolkit for Digital Safety Design Interventions and Innovations: Typology of Online Harms

Uma tipologia que fornece um quadro abrangente para os esforços da promoção da cibersegurança, ajudando na compreensão dos diferentes tipos de danos online e que permite trabalhar em colaboração para desenvolver políticas, intervenções e inovações rumo a um ecossistema digital mais seguro, respeitando direitos humanos e comportamentos positivos.

A tipologia procura atenuar as diferentes interpretações entre as partes interessadas (*stakeholders*), categorizando os danos para obter uma abordagem colaborativa e respeitadora dos direitos na segurança digital.

A typology that provides a comprehensive framework for cybersecurity promotion efforts, helping understand the different types of online harms and enabling collaborative work to develop policies, interventions and innovations towards a safer digital ecosystem, respecting human rights and positive behaviours.

The typology seeks to mitigate different interpretations among stakeholders by categorising harms to achieve a collaborative and rights-respecting approach to digital security.

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)
Krzysztof Hepner/Unsplash
Jean Philippe Delberghe/Unsplash

Publicação trimestral | Quarterly publication
Setembro 2023 | September 2023