bilingual edition

ptsoc {news}

Cibersegurança em 2023

3 perguntas a Sónia Martins

Compras online em segurança
por Luís Pisco

07

Cybersecurity in 2023

3 questions to Sónia Martins

Safe online shopping
by Luís Pisco

.pt

CIBERSEGURANÇA: TENDÊNCIAS PARA 2023

Protocolo de Cooperação .PT e Women4Cyber PT

11 de janeiro 2023 • edifício barra barra

Welcome coffee 16h30

Abertura 16h45

Luisa Ribeiro Lopes, .PT

Tertúlia 17h00

Ana Ferreira, CINTESIS@RISE/FMUP

Carla Zibreira, Axians

Inês Esteves, .PT

Sónia Martins, Núcleo de Cibercriminalidade, PSP

Moderação: *Fátima Caçador*

Encerramento 18h00

Cristina Almeida, W4C PT

Assinatura do Protocolo de Cooperação .PT e Women4Cyber PT

PRÓXIMOS EVENTOS

Workshop - Desafios & Boas Práticas de Segurança .PT e PSP
Roteiro INCoDe.2030 – Capacitação Digital
www.incode2030.gov.pt
Aveiro, 26 de janeiro 2023
Viana do Castelo, 9 de fevereiro 2023

Inovação, Conhecimento e Cibersegurança Protocolo de Cooperação .PT e Cisco Systems
16 de fevereiro 2023 • Edifício Barra Barra
Abertura | 16h30

Cibersegurança em 2023

Os inúmeros casos ocorridos em 2022 mostram que não foi um ano fácil para os responsáveis da cibersegurança nos setores público e privado. Mas poderá 2023 ser diferente?

O ano começou em Portugal com o mediático ataque à Impresa (Expresso e SIC), a que se seguiram a Vodafone Portugal, o Hospital Garcia da Horta, entidades de retalho e financeiras, laboratórios da saúde ou diferentes câmaras municipais, mais media (Lusa e Newsplex) e clubes desportivos, a TAP, o Estado-Maior das Forças Armadas ou a Segurança Social.

Cybersecurity in 2023

The numerous cases that occurred in 2022 show that it was not an easy year for those responsible for cybersecurity in both the public and private sectors. But could 2023 be different?

In Portugal, 2022 began with the media attack on the Impresa group (Expresso newspaper and SIC television network), followed by Vodafone Portugal, Garcia da Horta Hospital, retail and financial entities, health laboratories, several city councils, other media companies (Lusa news agency and Newsplex app) and sports clubs, TAP, the Portuguese Armed Forces General Staff or Social Security.

Os resultados mostram que não há um padrão: todas as áreas podem ser atacadas por indivíduos isolados ou grupos desconhecidos. Num "universo de adversários", por exemplo, o país contava apenas com o interesse de um grupo, o Cozy Bear, a atuar alegadamente em nome do Serviço de Inteligência Estrangeira da Federação Russa para disseminar "uma ampla gama de tipos de malware" em alvos específicos, com "repetidas tentativas de readquirir e estabelecer acesso a redes onde anteriormente perdera o controlo operacional".

"Em Portugal, no último ano, o panorama alterou-se substancialmente tendo-se assistido a um aumento muito significativo do número de ciberataques organizados a setores críticos como as telecomunicações, energia e saúde", reforça Ricardo Pires, gestor de cibersegurança do PTSOC.

"A democratização das novas tecnologias e a crescente digitalização das empresas e organizações trouxe para a sociedade novos riscos e ameaças que antes não eram consideradas", refere, quando "os cibercriminosos são mais organizados e proficientes na exploração de vulnerabilidades dos sistemas e aplicações".

Neste cenário, antecipa-se para 2023 "a necessidade de reforço contínuo da

The results show the absence of a pattern: all areas can be attacked by isolated individuals or unknown groups. In a 'universe of adversaries', for example, the country counted only on the interest of one group, Cozy Bear, allegedly acting on behalf of the Foreign Intelligence Service of the Russian Federation to disseminate 'an extensive range of malware types' on specific targets, with 'repeated attempts to re-acquire and establish access to networks where they had previously lost operational control'.

'In Portugal, over the last year, the panorama has changed substantially. There has been a very significant increase in the number of organised cyberattacks on critical sectors such as telecommunications, energy and health,' states Ricardo Pires, cybersecurity manager at PTSOC.

'The democratisation of new technologies and the increasing digitalisation of companies and organisations has brought new previously-unconsidered risks and threats to society', he says, when 'cybercriminals are more organised and proficient in exploiting vulnerabilities in systems and applications.'

In this scenario, 2023 is expected to 'need continuous reinforcement of cybersecurity in companies and organisations' in the face of the

cibersegurança nas empresas e organizações" perante o desenvolvimento de atividades como:

- Ransomware-as-a-service (RAAS): são ataques com uma tipologia de Content Distribution Network (CDN), semelhante à conhecida na distribuição de conteúdos de entretenimento, mas focados em disseminar malware. Tenderá a piorar em 2023 - nomeadamente para a obtenção de dados em instituições sanitárias - porque se "democratizou" o seu acesso, embora com uma nova estratégia de "Double-Extortion", em que, "para além de encriptar a informação, esta também é exfiltrada e são pedidos resgates para a desencriptar e para a não expor", nota Ricardo Pires. Para contrariar estes ataques, "as organizações devem implementar mecanismos como anti-malware, segmentação de redes, backups e um plano de continuidade de negócio".

- Tecnologias de IA na cibersegurança: ao prosseguir o investimento em Centros de Operações de Segurança (SOC), deve dar-se uma maior atenção às "soluções baseadas em inteligência artificial (IA) e de automação para otimizar o trabalho dos analistas de cibersegurança e melhorar o tempo de deteção e resposta a incidentes de segurança", prossegue Ricardo Pires.

development of activities such as:

- Ransomware-as-a-service (RAAS): These are Content Distribution Network (CDN) attacks, of a similar type to that known in the distribution of entertainment content. These, however, are focused on disseminating malware. It will tend to get worse in 2023 - namely to obtain data from health institutions - because its access has become 'democratised', although with a new 'Double-Extortion' strategy, in which, 'in addition to encrypting the information, it is also exfiltrated and ransoms are demanded to decrypt it and not expose it', notes Ricardo Pires. To counter these attacks, 'organisations should implement mechanisms such as anti-malware, network segmentation, backups and a business continuity plan.'

- AI technologies in cybersecurity: By continuing to invest in Security Operations Centres (SOCs), greater attention should be paid to 'artificial intelligence (AI) and automation-based solutions to optimise the work of cybersecurity analysts and improve detection and response time to security incidents,' Ricardo Pires continues.

- More demanding regulatory framework in data security and protection: The significant increase in cybercrime will

- Quadro regulatório mais exigente na segurança e proteção dos dados: o aumento significativo da cibercriminalidade levará, em 2023, "ao reforço da regulamentação nacional e europeia direcionada, trazendo em especial para as infraestruturas críticas e operadores de serviços essenciais novas obrigações e responsabilidades", antecipa o responsável do PTSOC.

- Competências nos domínios da cibersegurança: o phishing é "uma das maiores e mais antigas ameaças" à cibersegurança, mas continua a proliferar, salienta Ricardo Pires. Assim, é "fundamental que as organizações e empresas invistam fortemente em programas de sensibilização e formação dos seus colaboradores sobre os riscos e as boas práticas de cibersegurança".

O phishing, usando mensagens enganadoras de correio eletrónico, é um dos principais vetores para ciberataques às organizações, iludindo a capacidade humana para os evitar. É uma técnica que "joga com as emoções humanas. Mas consciencialização, reconhecimento, formação e tecnologia podem neutralizar os ataques mais sofisticados", reconhece também a revista CIO.

Para esta, há que reconhecer as diferenças entre os diferentes tipos de ataque, in 2023, 'to the strengthening of national and European targeted regulation, namely bringing new obligations and responsibilities to critical infrastructures and operators of essential services,' anticipates the PTSOC manager.

- Cybersecurity skills: Phishing is 'one of the biggest and oldest threats' to cybersecurity, but it continues to proliferate, stresses Ricardo Pires. It is therefore 'essential for organisations and companies to invest heavily in awareness and training programmes for their employees on cybersecurity risks and good practices.'

Phishing, using misleading email messages, is one of the main vectors for cyberattacks on organisations, deceiving the human capacity to avoid them. It is a technique that 'plays on human emotions. But awareness, recognition, training and tech can blunt the most sophisticated attacks,' CIO magazine also acknowledges.

For CIO, it is necessary to recognise the differences between the different types of attacks, from whaling to smishing or pharming, to train users to recognise and avoid attempted attacks and, as already mentioned, to use AI software both in training and in combating cyberattacks.

ques, do "whaling" ao "smishing" ou ao "pharming", formar os utilizadores para reconhecerem e evitarem as tentativas de ataques e, como já referido, usar software de IA tanto na formação como no combate aos ciberataques.

Nesse sentido, o metaverso é outro caso a necessitar de alguma atenção quando não se prospetiva a sua evolução e potencial para atividades criminosas mas se augura que algo se pode ali desenvolver. Para conhecer essas tendências, foi lançado o Interpol Metaverse para os utilizadores da polícia internacional. A mensagem deixada no lançamento é clara: "um universo virtual sem lei não será tolerado" "para a polícia perceber o metaverso, tem de o experienciar".

O fator humano

Uma abordagem a todas estas ameaças necessita de recursos humanos qualificados. A escassez de profissionais que se fez sentir em 2022 tenderá a prosseguir no próximo ano, porque a oferta académica e formativa não acompanha a enorme procura do mercado, com os técnicos a serem assediados nos campos empresarial e público.

A analista IDC considera que, para as TI em geral, "a escassez de capacidades críticas limitará os benefícios dos investimentos", quando "a maioria das em-

In that sense, the metaverse is another case in need of attention when one does not prospect its evolution and potential for criminal activities but foresees that something may develop there. To learn more about these trends, the Interpol Metaverse was launched for international police users. The message left at the launch is clear: 'a lawless virtual universe will not be tolerated' and 'in order for police to understand the Metaverse, we need to experience it.'

The human factor

An approach to all these threats needs skilled human resources. The shortage of professionals that was felt in 2022 will tend to continue next year, as the academic and training supply does not keep up with the huge market demand, with technicians being harassed in the corporate and public sectors.

Analyst IDC reckons that, for IT in general, 'shortages in critical skills will limit the benefits from IT investments,' when 'most companies will struggle to keep and find employees with the right skills, effectively putting more pressure on remaining employees to meet expanding digital business requirements.'

One estimate put the global cybersecurity workforce at 4.7 million people - 464 000 of whom entered the

presas tentará manter e encontrar funcionários com as capacidades certas, colocando efetivamente mais pressão sobre os funcionários remanescentes para atender aos crescentes requisitos dos negócios digitais".

market last year - a number that still falls short of the 3.4 million needed to fill the job vacancies in this area.

The market may be further disrupted by the anticipated path of the

Uma estimativa calculou a força de trabalho global na cibersegurança em 4,7 milhões de pessoas - das quais 464 mil chegaram ao mercado no ano passado - mas faltam ainda 3,4 milhões para preencher o número de vagas de emprego nesta área.

O mercado pode ser perturbado ainda mais pelo antecipado caminho da indús-

cybersecurity industry into 'a period of rapid consolidation,' as the interests of private investment funds and large companies in the market come together to try to offer comprehensive solutions to customers. It remains to be proven that a single vendor is the ideal answer, but organisations are worn down by having to deal with segmented and not always interoperable offers.

tria da cibersegurança para "um período de rápida consolidação", com a junção dos interesses de fundos de investimento privado e das grandes empresas do mercado que vão tentar oferecer soluções abrangentes aos clientes. Está por provar que um único fornecedor seja a resposta ideal, mas as organizações estão desgastadas por terem de lidar com ofertas segmentadas e nem sempre interoperáveis.

Até ao terceiro trimestre do ano, estas fusões e aquisições atingiram um valor de mais de 110 mil milhões de euros, bem acima dos cerca de 80 mil milhões de 2021, estimou um banco de investimento focado na cibersegurança.

Para o próximo ano, a Gartner antecipa uma despesa global de mais de 185 mil milhões de euros em produtos e serviços de segurança da informação e gestão de risco. Este valor deve subir para mais de 250 mil milhões em 2026 e os três principais fatores subjacentes ao crescimento são o trabalho remoto e híbrido, o abandono das VPNs para o acesso "zero trust" em redes e a oferta de modelos baseados em cloud, sendo esta "a categoria mais forte de crescimento em 2023".

Tendências em foco

2023 deve ser um ano de tolerância zero ("zero trust"), perante a generalização

By this year's Q3, these mergers and acquisitions reached more than €110bn, well higher than the close to €80bn in 2021, as estimated by an investment bank focused on cybersecurity.

For next year, Gartner anticipates a global spending of more than €185 billion on information security and risk management products and services. This figure is expected to rise to more than €250bn by 2026 and the three main factors fuelling the growth are remote and hybrid work, the transition from VPNs to zero trust network access and a shift to cloud-based models, this being the 'strongest category for growth in 2023'.

Trends in focus

2023 should be a zero trust year in the face of widespread threats derived from hybrid work models, in the office and at home. In the US, the federal government's recommendation for public administration is to adopt a zero trust policy by 2024 - a proposal that will tend to be followed by the private sector.

The activities most exposed to danger are the traditional critical infrastructures (water, electricity, health, telecommunications) but also defence, due to the war in Europe. The origin of the threats could come from

das ameaças derivadas dos modelos híbridos de trabalho, no escritório e em casa. Nos EUA, a recomendação do governo federal para a Administração Pública é a de adotar uma política "zero trust" até 2024 - uma proposta que tenderá a ser seguida pelo setor privado.

As atividades mais expostas ao perigo são as tradicionais das infraestruturas críticas (água, eletricidade, saúde, telecomunicações) mas também a defesa, devido à guerra na Europa. A origem das ameaças tanto poderá vir da espionagem estrangeira, de operações disfarçadas de hacktivismo como de ataques de botnets coordenadas para DDoS, tentando obter dados pessoais sensíveis, numa amálgama entre físico e virtual, entre atores civis e ciberoperações militares.

A Cybersecurity and Infrastructure Security Agency (CISA) também anunciou que se pretende focar na cibersegurança da infraestrutura de hospitais, escolas e setor da água no próximo ano. Os esforços da agência norte-americana foram detalhados em 37 metas voluntárias e não-exaustivas que procuram conciliar "custo, complexidade e impacto das iniciativas". Apenas três implicam elevados custo, impacto e complexidade: "proibir a conexão de dispositivos não autorizados; a validação por terceiros da eficácia de cibercontrolos e segmentação da rede".

foreign espionage, from operations disguised as hacktivism or from botnet attacks coordinated for DDoS, trying to obtain sensitive personal data, in an amalgamation between physical and virtual, between civilian actors and military cyber-operations.

The Cybersecurity and Infrastructure Security Agency (CISA) also announced that, next year, it intends to focus on the cybersecurity of infrastructure in hospitals, schools and the water sector. The US agency's efforts were detailed in 37 voluntary and non-exhaustive goals that seek to reconcile 'cost, complexity and impact of security initiatives.' Only three involve high cost, impact and complexity: 'prohibiting the connection of unauthorised devices; third-party validation of the effectiveness of cyber controls; and network segmentation.'

Other actions to watch out for when it comes to possibilities of cyberattack include the use of video or audio deepfakes to transfer financial data (personal or corporate), attempts to disrupt supply chains, vulnerabilities in autonomous vehicles, with attacks to the electronic systems of the growing fleet of these cars, and vulnerabilities in the increasingly widespread Internet of Things (IoT).

The latter show the opportunism of

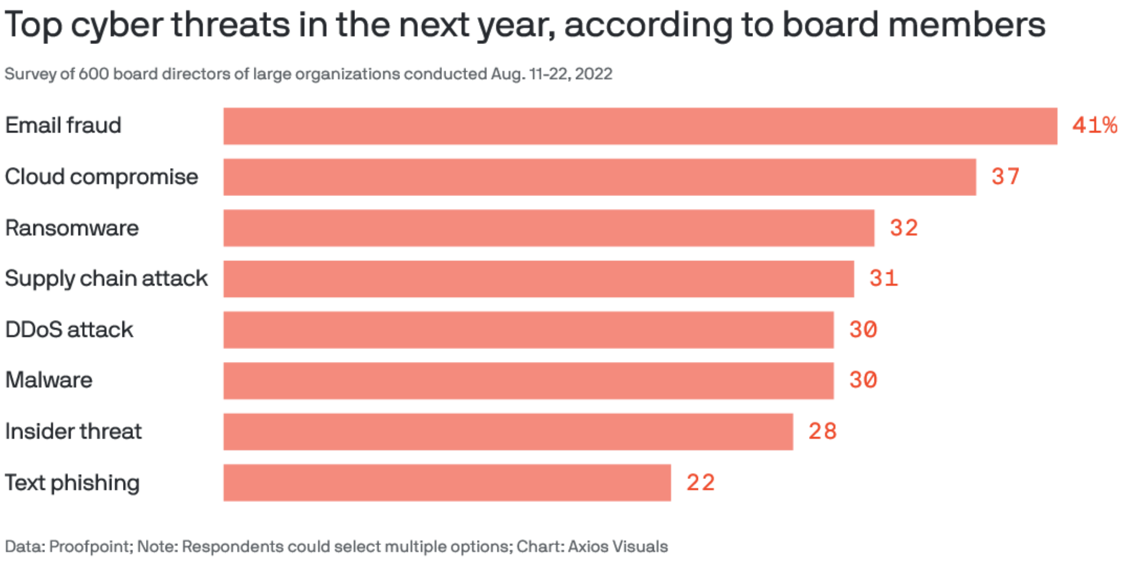
Outras ações a ter em atenção no registo das possibilidades de ciberataques passam pelo uso de "deepfakes" de vídeo ou áudio para a transferência de dados financeiros (pessoais ou empresariais), tentativas de disrupção das cadeias de fornecimento, as vulnerabilidades nos veículos autónomos, com ataques aos sistemas eletrónicos da crescente frota destes automóveis, e as vulnerabilidades na cada vez mais disseminada Internet das Coisas (IoT).

Estas últimas demonstram o oportunismo dos cibercriminosos em aproveitar as tecnologias mais recentes e com maior procura. Mas o mesmo pode ser dito perante as soluções que estão a surgir no mercado adotando tecnologias recentes para contrariar essas pretensões ilegais. Olhando para as 10 tendências tecnológicas estratégicas da Gartner para 2023, por exemplo, constam o "sistema imunológico digital", uma experiência que combina várias estratégias de software para proteção contra riscos por forma a "oferecer sistemas resilientes que atenuam os riscos operacionais e de segurança". No lado da gestão da confiança, risco e segurança por inteligência artificial (AI Trust, Risk and Security Management ou AI TRISM), combinam-se "métodos para explicar os resultados da IA, implantando rapidamente novos modelos, gerindo ativamente a segurança da IA e controlos para questões de privacidade e ética".

cybercriminals, by taking advantage of the latest and most popular technologies. But the same can be said in the face of solutions that are emerging in the market adopting recent technologies to counter these illegal claims. Looking at Gartner's 10 strategic technology trends for 2023, for example, are the 'digital immune system', an experiment that combines various software strategies for risk protection to 'deliver resilient systems that mitigate operational and security risks.' On the AI Trust, Risk and Security Management (AI TRISM) side, they combine 'methods for explaining AI results, rapidly deploying new models, actively managing AI security and controls for privacy and ethics issues.'

Adaptive AI, too, 'unlike traditional AI systems, can revise its own code to adjust to real-world changes not known or anticipated when the code was first written. Organisations that build adaptability and resilience into their design in this way can react more quickly and effectively to disruptions.'

These new propositions pave the way for innovative solutions not yet on the radar of decision-makers stuck in more traditional models. For example, a survey of 600 board directors from worldwide organisations with more than 5 000 employees conducted this year showed that their top fear for 2023 was email



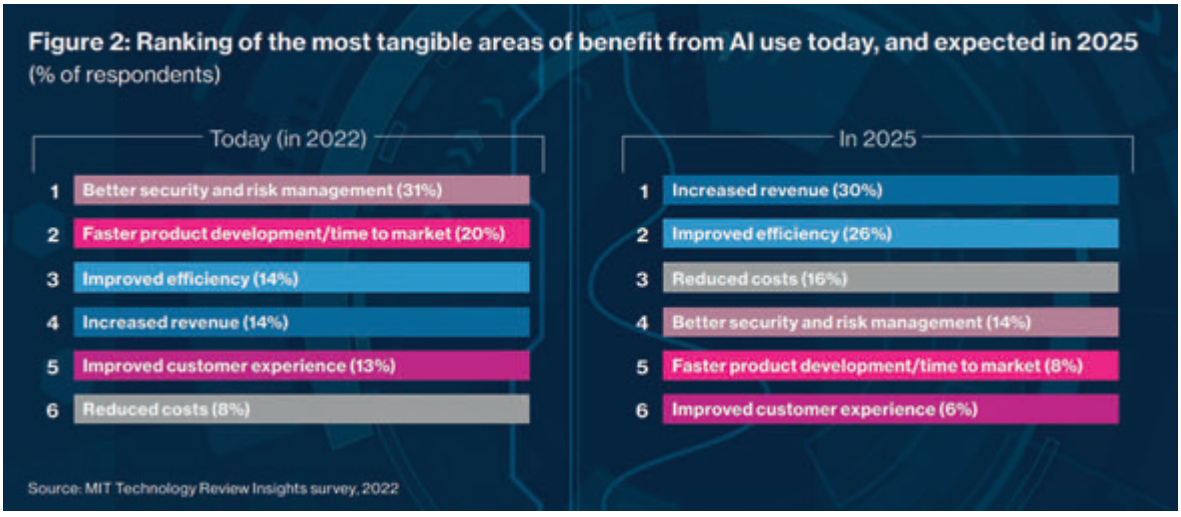
Também a IA adaptativa, "ao contrário dos sistemas tradicionais de IA, pode rever o seu próprio código para se ajustar às mudanças do mundo real que não eram conhecidas ou previstas quando o código foi escrito pela primeira vez. As organizações que criam adaptabilidade e resiliência no design desta maneira podem reagir de maneira mais rápida e eficaz às interrupções".

Estas novas propostas abrem caminho a soluções inovadoras que não estão ainda no radar dos decisores, presos a modelos mais tradicionais. Por exemplo, um inquérito a 600 executivos de organizações globais com mais de 5.000 funcionários, realizado este ano, mostrou que o seu principal temor para 2023 era a fraude por email (41%), enquanto do lado dos CISOs se ficava pelos 30%. Nos prin-

fraud (41 %), compared to 30 % of CISOs. This was followed by cloud compromise, ransomware and various types of attacks (supply chain, DDoS or malware).

If the answers in the 'CIO vision 2025' report are to be trusted, the area that benefits the most from the use of AI today is security and risk management. However, by 2025, growing revenues, more efficiency and cost reduction are expected to be 'the most tangible form of return gained from AI', followed by cybersecurity.

In the future, Google's security experts point to four predictions that should materialise within the next 5 to 10 years. The first involves technology convergence simplifying the security domain. 'Security controls mandated in



cipais receios, seguiam-se os serviços comprometidos de cloud, o ransomware e diversos tipos de ataques (à cadeia de fornecimento, de DDoS ou de malware).

A acreditar nas respostas do relatório "CIO vision 2025", a área que mais beneficia do uso da IA atualmente é a segurança e gestão de risco. No entanto, até 2025, espera-se que as crescentes receitas, mais eficiência e redução de custos sejam "a forma mais tangível de retorno obtida com a IA", seguindo-se então a cibersegurança.

Para o futuro, os responsáveis de segurança na Google apontam quatro previsões que se devem materializar nos próximo cinco a 10 anos. A primeira passa pela convergência tecnológica a simplificar o domínio da segurança. "Os controlos de segurança exigidos em regulamentos e estruturas de conformidade

regulations and compliance frameworks are going to be built, by default, into all of the widely used operating systems and enterprise systems,' says Heather Adkins, VP of Google's security engineering. 'The reality is that everyone's going to be hacked at some point, and the differentiator will become how quickly we recover from that,' Adkins said.

As for cloud infrastructure security, consistent updates based on data from vulnerability and threat research will turn it into a 'digital immune system'. Security updates will 'start to make some of these attacks fairly irrelevant', Adkins anticipates.

A third prediction is greater integration of security layers into every individual's 'experience with technology', with the automation of security updates, but also 'work on the human safety, not

serão incorporados, por defeito, em todos os sistemas operativos e sistemas corporativos amplamente usados", refere Heather Adkins, vice-presidente de engenharia de segurança da empresa. "A realidade é que todos vão ser 'hackados' nalgum momento, e o diferenciador será a rapidez com que se recupera disso".

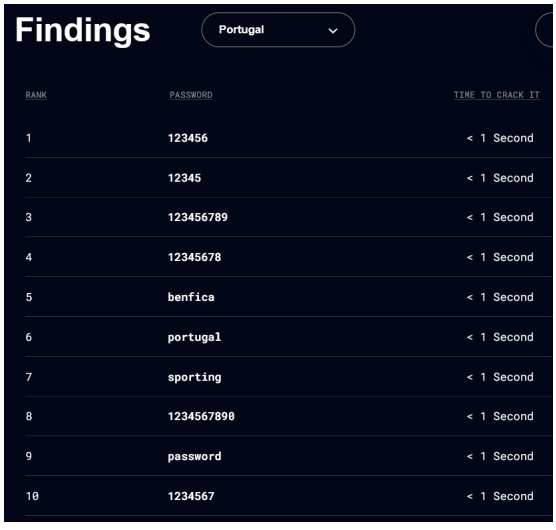
Quanto à segurança da infraestrutura de cloud, atualizações consistentes a partir da análise de dados das pesquisas de vulnerabilidades e de ameaças, vão transformar a cloud num "sistema imunológico digital". As atualizações de segurança vão "tornar alguns desses ataques bastante irrelevantes", antecipa Adkins.

Uma terceira vertente é uma maior integração de camadas de segurança em qualquer "experiência com tecnologia", com a automatização de actualizações de segurança, mas também "trabalhar na segurança humana, não apenas nos fundamentos técnicos", afirma Royal Hansen, vice-presidente de privacidade e segurança na Google.

Por fim, chegará "a morte das passwords" e aumentará a qualidade da autenticação para indivíduos e empresas. De forma consistente e ao longo de vários anos, a insegurança da autenticação manteve-se na escolha das palavras-passe e 2022 não foi diferente. A nível global, essa lista continuou a ser liderada por

just the technical underpinnings', says Royal Hansen, VP of privacy, safety and security at Google.

Eventually, we will see the 'death of passwords', and quality of authentication for individuals and businesses will increase. Consistently and over several years, authentication insecurity remained in the choice of passwords and 2022 was no different. Globally, that list continued to be led by password, 123456 and 123456789. In Portugal, the 10 most used passwords include variations of the 123456789 number sequence, interspersed with benfica, portugal, sporting and password.



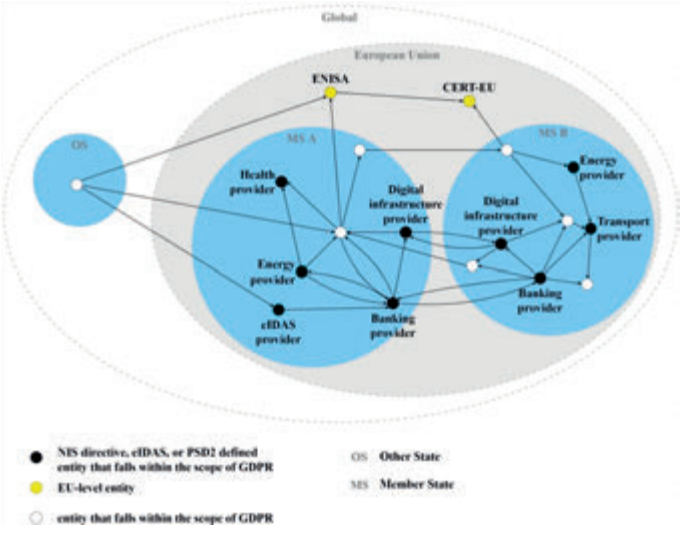
The European Union Agency for Cybersecurity (ENISA) also listed a dozen threats in this sector by the end of the

password, 123456 e 123456789. Em Portugal, as 10 mais usadas incluem variações da sequência numérica 123456789, intercalada com benfica, portugal, sporting e password.

A agência europeia para a cibersegurança ENISA elencou igualmente uma dezena de ameaças neste setor até ao final da década, apontando desde cadeias de fornecimento comprometidas a potenciais abusos na IA, em que refere igualmente a escassez de competências. Neste caso, a coerência europeia na cibersegurança é mais problemática, detetou o trabalho "Analysis of the cybersecurity ecosystem in the European Union".

decade, highlighting from compromised supply chains to potential abuses in AI, in which it also mentions the shortage of skills. In this particular case, European coherence in cybersecurity is more problematic, the 'Analysis of the cybersecurity ecosystem in the European Union' paper concluded.

The authors conclude that 'there are stakeholders missing from the EU-level cybersecurity ecosystem, like eGovernment entities and organisations that are not in the specified categories of [operators of essential services] (OESs) and digital service providers (DSPs)], even though they offer important



Os autores concluem que "faltam partes interessadas no ecossistema da cibersegurança da UE, como entidades do e-governo e organizações que não estão nas categorias especificadas [de operadores de serviços essenciais (OESs) e fornecedores de serviços digitais (DSPs)], embora ofereçam serviços importantes para os cidadãos ou representem entidades económicas significativas (ou mesmo dominantes), cujo tempo de inatividade afeta visivelmente o [Mercado Único Digital] europeu".

As diretivas NIS2 e SRI resolvem parcialmente estas questões. "As tarefas e obrigações alargadas da ENISA ajudaram a reduzir a diferença de capacidades e recursos, mas o quadro legislativo complexo mantém-se", afirmam os investigadores.

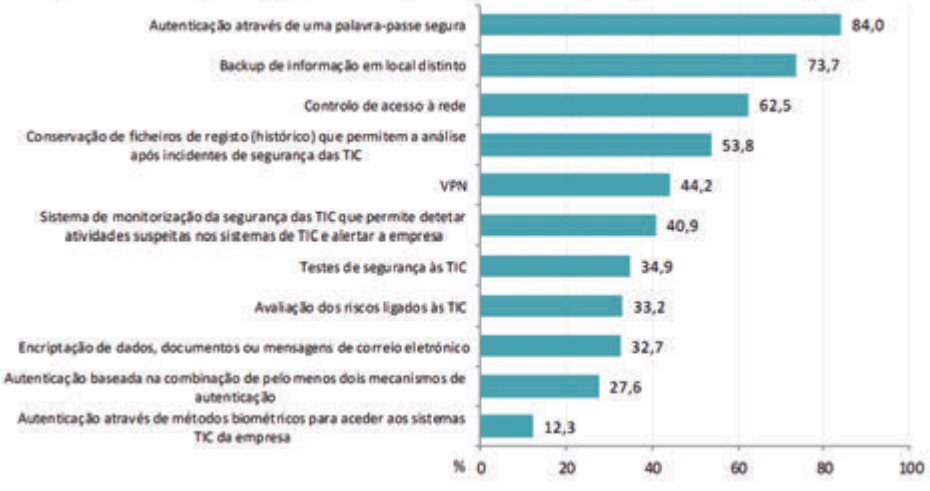
services for citizens or represent significant (or even dominant) economic entities, whose downtime visibly affects the European [Digital Single Market].'

The NIS2 and NIS directives partially resolve these issues, researchers say, and 'ENISA's expanded tasks and obligations have helped reduce the difference in capabilities and resources, but the complex legislative framework remains.'

Segurança das TIC em Portugal

ICT Security in Portugal

Figura 4.1. Empresas segundo as medidas de segurança das TIC utilizadas, em % do total de empresas com 10 ou mais pessoas ao serviço com ligação à internet para fins profissionais, por tipo de medidas e total (2022)



Fonte: INE, Inquérito à utilização de TIC nas empresas

A password é a principal medida de segurança utilizada por 84% das empresas nacionais, seguindo-se o backup de informação em local distinto (73,7%, em que se inclui colocá-la em cloud) e o controlo de acesso à rede (62,5%), referem os dados do Inquérito à Utilização de TIC nas Empresas - 2022, do INE.

Pouco mais de metade (53,8%) guarda um histórico da informação, o que facilita uma análise após incidentes de segurança das TIC. Neste domínio, a indisponibilidade de serviços foi a mais frequente (9,7% das empresas em 2021), seguida da destruição ou corrupção de dados (3,4%) e a divulgação de dados confidenciais (0,7%).

The password is the main security measure used by 84 % of national companies, followed by data back-up to a separate location (73.7 %, including placing it on a cloud) and network access control (62.5 %), according to data from the INE's Survey on ICT Use in Enterprises - 2022.

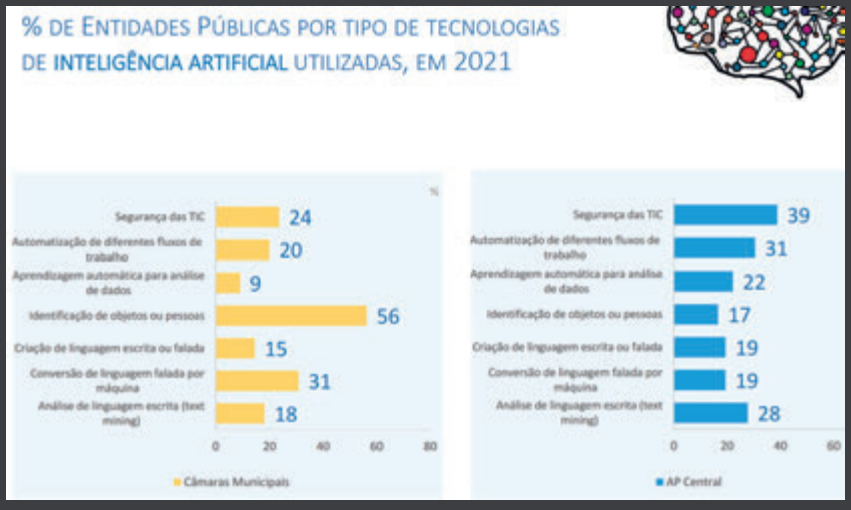
Just over half (53.8 %) keep a data history, which facilitates analysis after ICT security incidents. In this domain, unavailability of services was the most frequent (9.7 % of businesses in 2021), followed by destruction or corruption of data (3.4 %) and disclosure of confidential data (0.7 %).

Usos da IA na Administração Pública

Em 2021, as principais utilizações da inteligência artificial (IA) na Administração Pública Central foram na segurança das TIC (em 39% dos casos), seguindo-se a automatização de fluxos de trabalho e a análise de linguagem escrita. A IA foi usada na identificação de pessoas ou objetos em 56% das câmaras municipais, com a segurança a ser adotada em apenas 24%.

Uses of AI in Public Administration

In 2021, the main uses of artificial intelligence (AI) in Central Public Administration were in ICT security (in 39 % of cases), followed by workflow automation and written language analysis. AI was used in the identification of people or objects in 56 % of municipal councils, with security being adopted in only 24%.



Seguros de cibersegurança a crescer

O mercado global dos seguros de cibersegurança chegou quase aos 10 mil milhões de euros em 2021 e deve crescer a uma taxa anual composta (CAGR) de 19,29% entre 2022 e 2030.

Cybersecurity insurance on the rise

In 2021, the global cybersecurity insurance market reached almost €10bn and is expected to grow at a compound annual growth rate (CAGR) of 19.29 % between 2022 and 2030.

3

Sónia Martins

Chefe do Núcleo de Cibercriminalidade (NCIBER) do Departamento de Investigação Criminal da Direção Nacional da PSP
Head of the Cybercrime Unit, Criminal Investigation Department of the National Directorate of the Public Security Police (PSP)

1. Qual o balanço que o NCIBER faz de 2022? Destacou-se algum tipo de cibercriminalidade relativamente aos anos anteriores no Núcleo?

O NCIBER é um serviço da PSP, criado com o intuito de apoiar investigações da PSP a nível nacional, em que o recurso ao ciberespaço e o uso de 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 da competência de investigação da PSP, mas que agora recorrem a novos meios e a um novo espaço para o seu cometimento. Não se pode dizer que o nosso objeto sejam os cibercrimes informáticos puros. Todo o crime que acontece no ciberespaço é cibercrime, mas nem todo o cibercrime é crime informático. Existem crimes ciberinstrumentais e crimes ciberdependentes, a PSP atua essencialmente sobre os primeiros e/ou aqueles que forem delegados

1. What is the NCIBER's assessment of 2022, considering this type of crime in national territory? Did any type of cybercrime stand out compared to the previous three years of Centre operations?

The NCIBER is a service under the wing of the PSP, created with the purpose of supporting PSP's national investigations, in which the use of cyberspace, computers and technological means are instrumental to commit crimes. We are referring to the so-called 'traditional crimes', which have always existed, and which were already under PSP's investigative competence, but which are now being committed using new means and a new space. Our object is not solely pure cybercrime. Every crime that happens in cyberspace is considered a cybercrime, but not all cybercrimes are computer crimes. There are cyber-instrumental crimes and cyber-dependent crimes. The PSP acts mainly on the first and/or on those that are delegated by the Public Prosecution Service to the PSP.

Overall, cybercrime has been on the rise. What stands out from one year to the next is the way criminals act, the social engineering used and the dimension of some phenomena, like phishing.

2. Have you noticed if the many awareness campaigns for crimes such as phishing, for example, have had any

pelo Ministério Público.

O cibercrime, no geral, tem vindo a aumentar. O que se destaca de ano para ano é a alteração da forma de atuação dos criminosos, a engenharia social utilizada e ainda a dimensão de alguns fenómenos como o phishing.

2. Notaram que as diversas campanhas de sensibilização para crimes como o phishing, por exemplo, têm surtido algum efeito junto da população?

É essencial reforçar as campanhas de sensibilização e conteúdos didáticos no sentido de elevar o nível de conhecimento geral da população quanto a este tipo de crime. Isso passa, necessariamente, pela prevenção, sensibilização e esclarecimento da população.

Contudo, não dispomos de dados quantitativos que nos permitam com algum grau de certeza conhecer o nível de eficácia das ações, mas sabemos que em todas as realizadas há uma boa recetividade dos nossos interlocutores e há sempre alguém que nos diz que desconhecia este ou aquele aspeto. Isso significa para a PSP que a ação foi positiva, significa que houve alguém que ficou mais esclarecido e consciente e que poderá, em teoria, proteger-se melhor.

A PSP caracteriza-se, entre outros aspetos, por ser uma Polícia integral e de proximidade. Isto significa, por um lado, que existe uma preocupação em fazer face à criminali-

effect on the population?

It is paramount to strengthen awareness campaigns and educational content in order to raise the level of general knowledge regarding this type of crime. This necessarily involves prevention, awareness, and clarification of the population.

However, we do not have quantitative data to know, with some degree of certainty, how effective these initiatives are. We do know however that all initiatives carried out have a good receptivity from our interlocutors; someone always tells us that they did not know this or that aspect. For the PSP, this means that the initiative was positive, that there was someone who has been enlightened and aware, someone who could, in theory, protect themselves better.

The PSP is, among other things, an integral and community police. On the one hand, this means that there is a concern to deal with crime that affects citizens more directly. On the other hand, it also means that several community programmes have been created targeting specific audiences, such as the elderly, children or young people, to better suit them.

Considering cybercrime, we have sought to use this previous experience to adapt the campaigns to the phenomena we detect, to the most affected audiences and/or during certain times of the year, when these

dade que afeta mais diretamente o cidadão, mas também que foram sendo criados, ao longo dos anos, diversos programas de proximidade, visando públicos-alvo específicos, como idosos, crianças, jovens, com o intuito de criar campanhas adaptadas.

No contexto do cibercrime, temos procurado utilizar essa experiência anterior, para adaptar as campanhas aos fenómenos que vamos detetando, aos públicos-alvo mais afetados e/ou a determinadas épocas do ano, em que esses fenómenos se tornam mais expressivos - por exemplo, as burlas relacionadas com a venda de artigos online junto à época natalícia ou aquando do "Black Friday".

Existem serviços na PSP que se dedicam a analisar as denúncias que são recebidas diariamente, com o objetivo de mais facilmente detetar fenómenos emergentes e padrões de atuação dos criminosos, sendo essa informação de extrema importância para orientar quer a investigação, quer a prevenção da criminalidade.

Por último, realço o empenho que a PSP tem tido no estabelecimento de parcerias com outras instituições, bem como, na cooperação policial nacional e internacional. A título de exemplos refiro uma campanha de prevenção de falsos arrendamentos de imóveis, realizada em parceria com o Airbnb, e a participação num projeto internacional de prevenção da cibercriminalidade, com enfoque na dissuasão de potenciais criminosos en-

phenomena happen more often – like online shopping scams around the Christmas season or during Black Friday.

The PSP has services dedicated to analysing the complaints received daily, to detect emerging phenomena and criminals more easily. This information is extremely important to guide both the investigation and the prevention of crime.

Finally, I stress the commitment that the PSP has had in establishing partnerships with other institutions, and in its national and international cooperation with other police forces.

For example, in partnership with Airbnb, we carried out a campaign to prevent the lease of fake real estate. We also took part in an international project to prevent cybercrime with a focus on deterring potential criminals from taking the path of cybercrime. This project had a joint participation of the PSP, the PJ [Judiciary Police] and the CNCS [Portuguese National Cybersecurity Centre], which shows just how important networking is when it comes to facing such a global phenomenon.

3. How do you anticipate 2023 in terms of cybersecurity concerns, and how will the NCIBER's success be measured?

We anticipate a possible increase in phishing/ smishing/ vishing campaigns,

veredarem pelo caminho do cibercrime. Este projeto contou com uma participação conjunta da PSP, da PJ e do CNCS, o que denota a importância do trabalho em rede para fazer face a um fenómeno que é global.

3. Como antevê 2023, em termos de preocupações com a cibersegurança, e como se irá medir o sucesso do NCIBER?

Antevemos um possível aumento das campanhas de phishing/ smishing/ vishing cada vez mais sofisticadas e mais complexas.

De igual modo, prevemos que se manterá a tendência crescente dos últimos anos, relativamente a situações de burlas relacionadas com a utilização de plataformas online e criação de sites falsos.

O sucesso do NCIBER passa todos os dias pelo empenho da equipa que lá trabalha, mas passará também pelo empenho dos polícias que recebem as denúncias nas esquadras e interagem diretamente com o cidadão. Quanto melhor forem recolhidos os indícios numa primeira fase, melhor poderão os investigadores trabalhar, numa segunda fase. Por este motivo, tem havido uma aposta na formação interna dos polícias sobre estas matérias, começando pelos polícias que já trabalham em investigação criminal ou que estão a integrar essa estrutura e, a breve prazo, passará pela formação base dos polícias que ingressam nas carreiras de agentes, chefes e oficiais.

increasingly sophisticated and complex.

Likewise, we anticipate that the growing trend of recent years will continue, regarding fraud related to the use of online platforms and the creation of fake websites.

The NCIBER's success can be measured by the daily commitment of its team, but also by the commitment of the police officers who receive the complaints in the police stations and interact directly with citizens. The better any evidence is initially collected, the better researchers can do their job in the following stages. This is why there has been a focus on the internal training of police officers on these issues, starting with police officers already working in criminal investigation or who are part of this structure. In the short term, it will also include the basic training of police officers starting their careers as agents, chiefs and officers.

Luís Pisco

Jurista do Departamento Jurídico e Económico da DECO
Legal expert from DECO's Legal and Economic Department

Compras online em segurança

O Natal e os saldos são tradicionalmente épocas de forte apelo ao consumo, no qual os consumidores se encontram mais suscetíveis a serem persuadidos a comprar, muitas vezes por impulso e sem a necessária reflexão. As compras online são, assim, uma excelente opção para quem pretende comparar as diferentes ofertas e fazer as suas compras de forma cómoda e rápida. Mas devemos ter alguns cuidados:

Escolha lojas online de confiança

De forma a reduzir os riscos de ser enganado, o consumidor deve escolher apenas vendedores que lhe ofereçam alguma confiança, nomeadamente aqueles cujo website disponibiliza a sua morada física e outras formas de contacto (fundamentais para efeitos de uma reclamação, por exemplo), bem como outra informação sobre o vendedor (um vendedor idóneo nada tem a esconder) e sobre a sua política de privacidade e segurança (informação sobre a política dos dados pessoais dos clientes).

Safe online shopping

Traditionally, Christmas and sales are times of strong consumer appeal, when consumers are more likely to be persuaded to buy, often on impulse and without the necessary reflection. Online shopping is therefore an excellent option for those who want to compare different offers and do their shopping conveniently and quickly. But we must be careful:

Choose trustworthy online shops

To reduce the risks of being deceived, consumers should only choose sellers they consider to be of trust, namely those whose website provides their physical address and other form of contact (essential for complaint purposes, for example), as well as other information about the seller (a reputable seller has nothing to hide) and their privacy and security policy (information about the customers' personal data policy).

Created precisely to give consumers more confidence, the CONFIO trustmark is an accreditation process that awards

Criado exatamente para dar mais confiança aos consumidores, o Selo CONFIO é um processo de acreditação que atribui este selo aos websites aderentes que cumpram um conjunto de regras e boas práticas relativas ao comércio eletrónico estabelecidas no seu código de conduta, tornando mais seguras as compras online.

Antes de comprar, compare preços

Antes de comprar é essencial que o consumidor compare preços, uma vez que estes poderão ser diferentes, consoante o vendedor, a plataforma utilizada ou se incluem ou não, os portes de envio. Para esse efeito existem na Internet vários comparadores de preços, que permitem comparar os preços de uma grande variedade de produtos e de lojas online.

Seja como for, devemos desconfiar sempre de preços e ofertas demasiado boas para serem verdade! Se os vendedores nos forem desconhecidos e as ofertas ou promoções forem demasiado aliciantes, muito abaixo do preço de mercado, geralmente são sinais de alerta de se tratar de um esquema fraudulento ou venda de produtos não genuínos.

Procure no site informação sobre os seus direitos

De acordo com a lei em vigor, as lojas on-

this trustmark to websites that comply with a set of e-commerce rules and good practices established in their code of conduct, making online shopping safer.

Compare prices before buying

Before buying, it is essential that you compare prices, as they may differ depending on the seller, the platform used and whether or not they include shipping costs. Given this, there are several price comparators available online, which allow us to compare the prices of a wide variety of products and online shops.

In any case, we should always be suspicious of prices and offers that are too good to be true! If we do not know a given seller, of if a promotion is too enticing, too far below the market price, these are usually warning signs of a fraudulent scheme or that you are dealing with the sale of fake products.

Search the website for information about your rights

Pursuant to current law, online shops should provide consumers with information about their rights, namely how the contracting process takes place, terms and delivery costs, how to file a complaint, warranty periods, how the refund or exchange of products

line devem disponibilizar aos consumidores informação sobre os seus direitos, designadamente, como decorre o processo de contratação, termos e custos de entrega, como devem proceder em caso de reclamações, quais os prazos de garantia, como se processa o reembolso ou a troca de produtos, ou informação sobre o direito de livre resolução e forma do seu exercício pelo consumidor. Com efeito, um dos direitos mais importantes dos consumidores que compram online a um vendedor domiciliado na UE é exatamente o direito de poder livremente resolver (anular) a compra e venda e exigir o reembolso do preço pago, no prazo de 14 dias.

Cuidados a ter no pagamento

Depois de adicionar ao "carrinho de compras" todos os produtos que quer comprar, segue-se o pagamento. Nesta fase, o consumidor deve verificar se se encontra numa página encriptada, por exemplo verificando se existe o símbolo de um pequeno cadeado na barra de endereços do seu browser e se o endereço da página web do vendedor começa com "https://". Tal significa que está a ser usada encriptação que impede que certos dados sensíveis como credenciais da conta, por exemplo, não serão enviados. No entanto, apesar desta aparente segurança, o consumidor deve ter consciência que não existe uma garantia de

is processed, or information about the right of free resolution and how consumers can resort to it. In fact, one of the most important rights for consumers buying online from an EU-based seller is precisely the right to freely withdraw from the purchase and sale and claim a refund of the price paid, within 14 days.

Cautions on payment

After adding all the products you want to buy to your cart, the next step is payment. At this stage, consumers should check whether they are on an encrypted page, for example by checking that there is a small padlock symbol in their browser's address bar, and that the address of the seller's webpage begins with 'https://'. This means that encryption is being used which prevents certain sensitive data such as account credentials, for example, from being sent. However, despite this apparent security, consumers should be aware that there is no absolute guarantee of security, hence the importance of choosing a good seller.

To complete the purchase, consumers should only provide the data necessary for its completion. Do not share unnecessary personal data.

Among the means of payment made available by the seller, avoid using a

Fonte: DECO

segurança absoluta, daí a importância da escolha do vendedor.

Para concluir a compra, o consumidor deve apenas fornecer os dados necessários à sua conclusão. Não partilhe dados pessoais desnecessários.

Entre os meios de pagamento disponibilizados pelo vendedor, evite utilizar o cartão de crédito em sites nos quais nunca fez compras antes, preferindo a utilização de cartões virtuais ou pagamento por multibanco.

credit card on websites where you have never shopped before, preferring the use of virtual cards or payment by ATM reference.

Radar das tecnologias de segurança

Uma análise a mais de 150 tendências da cibersegurança permitiu gerar este Cyber Tech Radar, com oito domínios críticos para a gestão e níveis de maturidade entre as que podem ser adotadas rapidamente ou a mais de cinco anos. Estas tendências revelam a "velocidade de inovação" a nível empresarial, mas também dos cibercriminosos, que não deixam ninguém à margem de poder ser atacado.

Security Tech Radar

An analysis of more than 150 cybersecurity trends has generated this Cyber Tech Radar with 8 critical areas for management and maturity levels between those that can be adopted quickly or that can take five years and above. These trends reveal the 'speed of innovation' at the enterprise level, but also of cybercriminals, where no one is safe from being attacked.

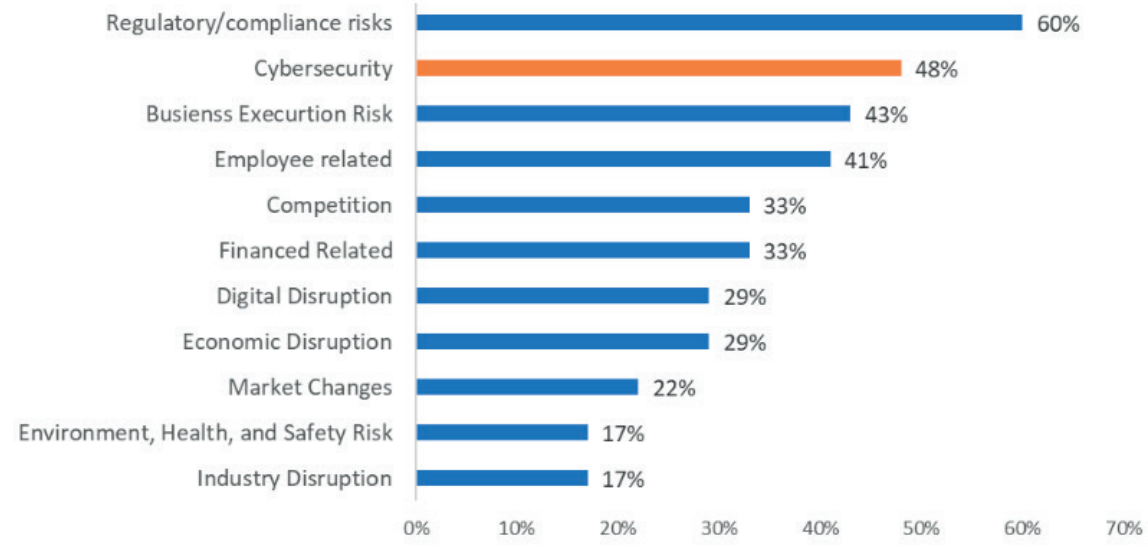
Deep Web com má imprensa

A imprensa tende a dar uma imagem negativa da Deep Web. Ela é "predominantemente associada ao crime, mercados criptográficos e conteúdo imoral, enquanto os usos positivos da tecnologia, como proteger a privacidade e a liberdade de expressão, foram amplamente desconsiderados".

Deep Web gets bad press

The press tends to give the Deep Web a negative image. It is 'predominantly associated with crime, crypto markets and immoral content, while positive uses of this technology, such as protecting privacy and freedom of speech, were largely disregarded'.

Figure 1: Top sources of risk to the enterprises



Europa quer plataforma de investimento

O crescimento da Internet, das soluções baseadas em cloud, dos dispositivos ligados e serviços online fez aumentar a exposição às ciberameaças e o custo anual do cibercrime na economia global foi estimado em €5,5 biliões em 2020, segundo o "European Cybersecurity Investment Platform" publicado pelo Banco Europeu de Investimento. Este relatório procura avaliar a oportunidade de criar um veículo financeiro para apoiar o ecossistema de cibersegurança na União Europeia e reduzir a dependência de outros mercados geopolíticos após ter detetado lacunas no investimento.

Europe wants investment platform

The growth of the Internet, cloud-based solutions, connected devices and online services has increased exposure to cyber threats. The annual cost of cybercrime to the global economy has been estimated at €5.5 trillion by 2020, according to the 'European Cybersecurity Investment Platform' published by the European Investment Bank. This report seeks to assess the opportunity to create a financial vehicle to support the cybersecurity ecosystem in the European Union and reduce reliance on other geopolitical markets after finding investment gaps.

Mapa dos ataques de ransomware

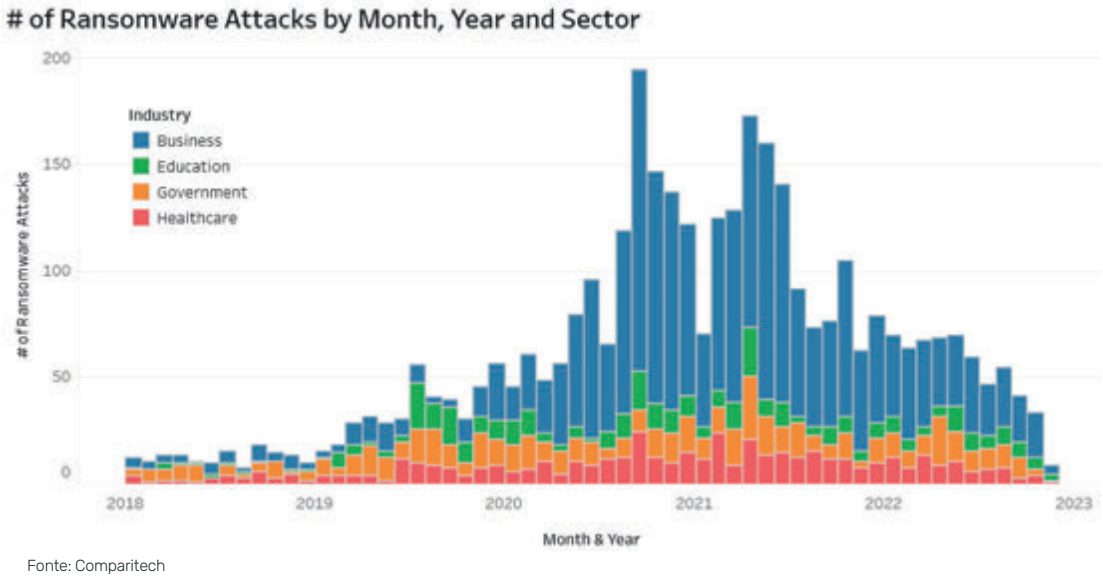
Uma ferramenta com atualização diária dos ataques de ransomware por setor (saúde, educação, governo e empresarial), com registos desde 2018, confirma como estes ataques prosseguem mas em menor número do que os registados no ano passado.

Mas se a quantidade diminuiu, aumentou o valor dos resgates pedidos e diversificaram-se os setores afetados, incluindo o da educação, que levou o FBI a emitir um alerta sobre a venda de credenciais de instituições do ensino superior em mercados e fóruns online ilegais.

Map of ransomware attacks

An updated tool of ransomware attacks by sector (health, education, government and enterprise), with records going back to 2018, it confirms how these attacks continue albeit in smaller numbers than those recorded last year.

But if the number of attacks has decreased, the amount of ransoms requested has increased and the sectors affected have diversified, including education, which led the FBI to issue an alert on the sale of credentials from higher education institutions on illegal online marketplaces and forums.



Fonte: Comparitech

Directora | 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)
Benjamin Suter | Unsplash
Steven Ramon | Unsplash

Publicação trimestral | Quarterly publication
Dezembro 2022 | December 2022