bilingual edition

ptsoc{news}

12

Cibersegurança da cloud

3 perguntas a Marcos Eckart Esteves

Ciberataques e comunicação segura por Vasco Sampaio

Cloud cybersecurity

3 questions to Marcos Eckart Esteves

Cyberattacks and safe communications by Vasco Sampaio

.pt

Cibersegurança da cloud

A segurança dos centros de dados que fornecem serviços em nuvem (cloud) é um tema incontornável, nomeadamente para quem os gere diariamente ou para quem paga pelo serviço. Nos EUA, em fevereiro passado, a Cloud Security Alliance (CSA) apresentou os resultados de um inquérito a mais de 2.000 profissionais das TI, com 77% a declarar estar pouco preparado para lidar com as ciberameaças e 18% das organizações assumiu que demora mais de quatro dias a resolver vulnerabilidades críticas.

Perante a dificuldade em manter a confiança entre os envolvidos, num ambiente de ligações à Internet sempre ativas e seguras, a responsabilidade na segurança dos dados tem de ser garantida pelos fornecedores dos serviços em cloud, amparadas por boas práticas dos clientes.

"Os serviços de cloud são complexos e, portanto, a sua segurança é um problema multi-facetado", explica Miguel Pupo Correia, professor do Instituto Superior Técnico/INESC-ID. A referida CSA "periodicamente publica documentos sobre as principais ameaças aos serviços em cloud. O mais recente, 'Top Threats to Cloud Computing - Pandemic Eleven' de 2022, apresenta 11 ameaças/vulnerabilidades".

No topo das preocupações está "o controle de acesso às funcionalidades de admi-

Cloud cybersecurity

The security of data centres that provide cloud services is an unavoidable issue, particularly for those who manage them daily or pay for its service. Last February, in the US, the Cloud Security Alliance (CSA) presented the results of a survey carried out to more than 2 000 IT professionals, where 77 % declared they felt unprepared to deal with cyberthreats and 18 % of organisations assumed that it takes more than four days to address critical vulnerabilities.

Faced with the difficulty of maintaining trust between those involved, in an environment where Internet connections are always secure and on, responsibility for data security must be guaranteed by cloud service providers, backed up by good customer practices.

'Cloud services are complex, which is why their security is a multi-faceted problem', explains Miguel Pupo Correia, professor at Instituto Superior Técnico/INESC-ID. CSA 'periodically publishes documents on the main threats to cloud computing. The latest one, 'Top Threats to Cloud Computing - Pandemic Eleven' from 2022, presents 11 threats/vulnerabilities.'

At the top of the list of concerns is 'access control to the service's administration functions. In conventional, non-cloud services, the company providing the

nistração do serviço. No caso dos serviços convencionais, não cloud, a empresa que fornece o serviço tem um canal de acesso privilegiado aos sistemas: o acesso físico. Pelo contrário, nos sistemas em cloud, a forma de acesso é idêntica para os fornecedores do serviço (clientes do fornecedor de cloud) e os eventuais adversários. Esta diferença torna crítico o controle do acesso às referidas funcionalidades de administração, pois se este for vulnerável, pode permitir o controle do sistema por parte de terceiros. Isso permite por exemplo o pedido de quantias de resgate, a sabotagem, o roubo de dados ou até a completa destruição do serviço. Aliás, já aconteceu várias vezes com resultados desastrosos, até com empresas portuguesas", recorda.

A mistura de procedimentos e de tecnologias que asseguram a cibersegurança na cloud passa muito por evitar essa "crise" na gestão de identidades e de acessos (IAM), por políticas de "governance" (para prevenção, deteção e atenuação de ameaças), garantir o planeamento na retenção e manutenção dos dados e continuidade do negócio, além das diferentes conformidades regulatórias e legais em, por vezes, diversas geografias e legislações.

O âmbito é mais vasto, por englobar a responsabilidade de proteção de todo o hardware e software, das redes físicas e da manutenção da energia elétrica, no lado do fornecedor dos serviços de cloud, mas tam-

service has a privileged access channel to the systems, a physical access. When it comes to cloud systems, access is carried out the same way by service providers (cloud provider customers) and by possible adversaries. This difference makes it critical to control access to these administration functions; if vulnerable, it could allow third parties to control the system. This could lead, for example, to ransom demands, sabotage, data theft or even the complete destruction of the service. In fact, this has happened several times with disastrous results, even with Portuguese companies,' Pupo Correia recalls.

The mix of procedures and technologies that ensure cloud cybersecurity includes avoiding this 'crisis' in identity and access management (IAM), governance policies (to prevent, detect and mitigate threats), ensuring planning in data retention and maintenance, and business continuity, as well as different regulatory and legal compliance in sometimes different geographies and legislations.

The scope is broader, as it encompasses the protection of all the hardware and software, the physical networks, and the maintenance of electrical power, on the side of the cloud service provider, as well as the analysis and guarantee of some security right down to the interface with the customer and its end users. It can be particularly difficult to manage this environment when the customer is a

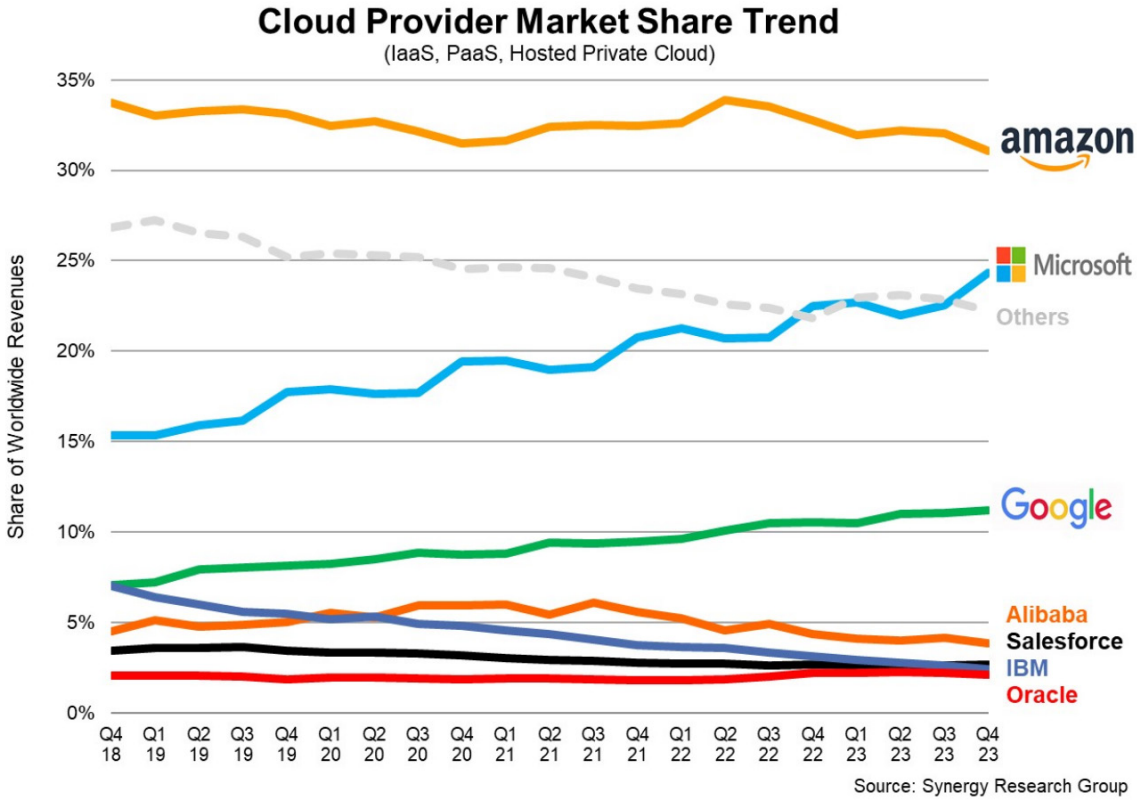
bém analisar e garantir alguma segurança até à interface com o cliente e os seus utilizadores finais. Em particular, a gestão deste ambiente é difícil quando o cliente são governos, como descobriu a Microsoft em 2023 num incidente com contas de email de responsáveis norte-americanos.

Difícil pode também ser a escolha no uso de fornecedores de serviços cloud. Pela sensibilidade dos dados, algumas organizações podem preferir fazer a gestão usando a sua própria infra-estrutura, assumindo muitos dos custos antes referidos e que são distribuídos pelos clientes em serviços de cloud.

government entity, as Microsoft discovered in 2023 with an incident involving the email accounts of US officials.

Choosing a cloud service provider can also be difficult. Due to the sensitivity of the data, some organisations may prefer to manage it using their own infrastructure, assuming many of the abovementioned costs which are distributed to cloud service customers.

The approach is to balance the results in terms of productivity and security, anticipating the reliability requirements to keep data safe, especially considering that



A abordagem passa por equilibrar os resultados na produtividade e na segurança, antecipando os requisitos de fiabilidade para manter os dados seguros, até porque a transferência da responsabilidade pela sua segurança não equivale a uma transferência total dessa mesma incumbência para o fornecedor dos serviços de cloud.

Os problemas são complexos, reforça Pupo Correia, e "têm de ser geridos, reduzindo o nível de vulnerabilidade do serviço, pela equipa de segurança da empresa que o fornece. Novas ameaças específicas irão necessariamente aparecer com o tempo, mas as grandes classes de ameaças parecem-me ser conhecidas".

Por exemplo, a transferência segura de dados entre serviços de cloud, por vezes entre diferentes ambientes regulatórios é um dos problemas "mais bem conhecidos e resolvidos. Hoje sabemos bem como garantir propriedades como a autenticidade, confidencialidade e integridade das comunicações. Existem protocolos padronizados para as garantir, como o TLS (Transport Layer Security). Já os riscos regulatórios são mais recentes e específicos do mundo da cloud. Esses existem sim, mas dependem da legislação nacional ou supra-nacional, como no nosso caso, em que estamos inseridos na União Europeia. Existem restrições de envio de certos dados para fora do país e da UE e a transparência fornecida pela cloud pode criar problemas. Por exemplo, uma empre-

transferring responsibility for its security is not the same as transferring it completely to the cloud service provider.

The problems are complex, emphasises Pupo Correia, and 'have to be managed by reducing the service's level of vulnerability by the security team of the company providing it. New specific threats will necessarily appear over time but, to me, the major classes of threat seem to be well known.'

For example, the secure transfer of data between cloud services, sometimes between different regulatory environments, is one of the 'best known and best solved' problems. Nowadays, we know how to safeguard properties such as authenticity, confidentiality and integrity of communications. There are standardised protocols to guarantee them, such as TLS (Transport Layer Security). Regulatory risks, on the other hand, are more recent and specific to the cloud world. These do exist, but they depend on national or supra-national legislation, as in our case, given we are part of the European Union. There are restrictions when it comes to sending certain data outside the country and the EU, and the transparency provided by the cloud can create problems. As an example, a company can place data in a cloud provider's data centre in Europe, but this provider can replicate (copy) that data outside the EU for reasons of fault tolerance without the client company becoming aware of it. These are

sa pode colocar dados num centro de dados de um fornecedor de cloud na Europa, mas este fornecedor pode replicar (copiar) esses dados fora da UE por uma questão de tolerância a faltas sem que a empresa cliente o note. É preciso cuidar esse tipo de questões de 'compliance'" (ver caixa "Desafios da segurança nas nuvens").

Desafios da segurança nas nuvens

- **Falta de visibilidade**: é fácil perder a noção de como os dados são acedidos e por quem, quando muitos serviços na cloud são acedidos fora das redes empresariais e por terceiros.
- **"Multitenancy":** os ambientes de cloud pública abrigam várias infraestruturas de clientes. É possível que os serviços alojados possam ser comprometidos por atacantes maliciosos ao visarem outras organizações.
- **Gestão de acessos e TI "sombra":** embora as organizações possam gerir e restringir os acessos nos seus sistemas "on-premise", a administração destes em cloud pode ser perigosa a quem permite acessos não filtrados a partir de qualquer dispositivo ou localização geográfica.
- **Conformidade ("compliance"):** a gestão da conformidade regulatória pode ser uma confusão para quem utiliza implementações de clouds públicas ou híbridas. A responsabilidade pela privacidade e segurança dos dados continua a ser da empresa, e a forte dependência de soluções de terceiros para gerir esta componente pode levar a problemas de conformidade dispendiosos.
- **Configurações incorretas:** parte da violação de registos pode ser atribuída a ativos mal configurados, que podem incluir não alterar as passwords de origem do fabricante ou a não criação de definições de privacidade adequadas. A responsabilidade por quaisquer violações de dados é quase sempre do proprietário dos mesmos.

Fonte: adaptado de texto da IBM

some of the compliance issues that need to be taken into consideration (see box 'Cloud security challenges').

Cost-benefit scenarios come up quite strongly in SME decisions as cloud computing can improve the security of assets to be preserved in a more tested

Challenges of cloud security

- **Lack of visibility:** It is easy to lose track of how data is accessed and by whom when many cloud services are accessed outside corporate networks and by third parties.
- **Multitenancy:** Public cloud environments house several customer infrastructures. It is possible that hosted services could be compromised by malicious attackers targeting other organisations.
- **Access management and 'shadow' IT:** Although organisations can manage and restrict access to their on-premise systems, administering them in the cloud can be dangerous for those who allow unfiltered access from any device or geographical location.
- **Compliance:** Managing regulatory compliance can be confusing for those using public or hybrid cloud deployments. Responsibility for data privacy and security remains with the company, and heavy reliance on third-party solutions to manage this component can lead to costly compliance problems.
- **Incorrect configurations:** Part of the breach of records can be attributed to poorly configured assets, which can include not changing the manufacturer's source passwords or not creating adequate privacy settings. Responsibility for any data breaches almost always lies with the data owner.

Source: adapted from an IBM text

Os cenários de custo-benefício colocam-se com alguma veemência nas decisões das PMEs porque a computação em cloud pode melhorar a segurança dos ativos a preservar num ambiente de cibersegurança mais testado, com soluções e recursos mais robustos. No entanto, uma falha neste ambiente compromete todas as organizações ali albergadas. Uma situação de maior conforto passa pelos clientes assegurarem auditorias de cibersegurança ao espaço em cloud onde residem os seus dados, complementando as efetuadas pelos fornecedores dos serviços. E, sabendo da grande quantidade de dados armazenados se transformam em "lixo" ao longo do tempo, uma boa prática é encriptar e limpar os repositórios de dados cuja re-utilização não se antevê para breve.

Para alguns gestores (financeiros ou de TI), pode ser mais confortável tê-los onde julgam deter um maior controlo sobre esses ativos e estarem em conformidade com obrigações regulatórias – nomeadamente em organizações obrigadas a conformidades multi-fornecedores, sedeados em diferentes regiões.

Estar atento às atualizações da informação prestada por entidades como o EU Cloud CoC (Europa) ou a Cloud Service Alliance nos EUA é igualmente pertinente. "Ambas realizam um papel muito importante de promoção da segurança de sistemas de cloud, a primeira com o foco na 'compliance' com o RGPD, a segunda de forma mais genérica. As equipas de segurança das empresas

cybersecurity environment, with more robust solutions and resources. However, a failure in this environment compromises all the organisations housed therein. A more comfortable situation is for customers to ensure cybersecurity audits of the cloud space where their data is stored, complementing those carried out by service providers. In addition, knowing that a large amount of stored data turns into 'junk' over time, a good practice is to encrypt and cleanse data repositories that are not expected to be re-used any time soon.

For some (financial or IT) managers, it may be more comfortable to have them where they believe they have greater control over these assets and are in compliance with regulatory obligations - namely, in organisations obliged to comply with multi-vendor agreements, based in different regions.

Keeping an eye on information updates provided by organisations such as the EU Cloud CoC (Europe) or the Cloud Service Alliance is equally pertinent. 'Both play a very important role in promoting the security of cloud systems, the former with a focus on compliance with the GDPR, the latter more broadly. The security teams of companies with cloud services should carefully follow the recommendations published by these organisations in order to continue to comply with best practices and remain attentive to the new challenges that arise,' recommends the IST professor.

que tenham serviços na cloud devem seguir atentamente as recomendações publicadas por essas entidades de modo a continuarem as seguir as melhores práticas e de permanecerem atentas aos novos desafios que vão surgindo", recomenda o professor do IST.

Por fim, alguma atenção é necessária nas fusões e aquisições de fornecedores de cloud (e de gestão de dados pessoais, em geral), porque se podem gerar situações conflituosas que levem a uma potencial usurpação de dados sensíveis.

Finally, attention should also be paid to mergers and acquisitions of cloud providers (and personal data management providers in general), as this can lead to conflicts and potential usurpation of sensitive data.

Parallel concerns

The security of complex cloud services 'is a multi-faceted problem', Pupo Correia explains. All the more so, as the amount of data continues to increase and cloud services are themselves third-party dependent, who

Modelos de serviços em cloud

- A computação em nuvem é assegurada pelos fornecedores destes serviços normalmente em modelos de IaaS, PaaS e SaaS.
- O primeiro, Infrastructure-as-a-Service, junta a gestão parcelar de dados e aplicações dos clientes com a gestão de hardware, redes e necessidades de armazenamento pelos fornecedores de cloud.
- A PaaS (ou Platform-as-a-Service) agiliza o processo de desenvolvimento e teste de aplicações, assegurando atualizações de software ou da infraestrutura em cloud.
- Por fim, o modelo SaaS (Software-as-a-Service) disponibiliza software online e normalmente por assinatura.

Cloud service models

- Cloud computing is provided by the suppliers of these services, usually in IaaS, PaaS and SaaS models.
- The first, Infrastructure-as-a-Service, combines the piecemeal management of customer data and applications with the management of hardware, networks and storage needs by cloud providers.
- PaaS (Platform-as-a-Service) streamlines the application development and testing process, ensuring software or cloud infrastructure updates.
- Finally, the SaaS (Software-as-a-Service) model makes software available online, usually on a subscription basis.

Service Type	Vendor Responsibility	User Responsibility
SaaS	Application security	Endpoints, user and network security Misconfigurations, workloads and data
PaaS	Platform security, including all hardware and software	Security of applications developed on the platform Endpoints, user and network security, and workloads
IaaS	Security of all infrastructure components	Security of any application installed on the infrastructure (e.g. OS, applications, middleware) Endpoints, user and network security, workloads, and data

Fonte: CrowdStrike

Preocupações paralelas

A segurança dos complexos serviços de cloud "é um problema multi-facetado", como explicou Pupo Correia. Tanto mais quanto a quantidade de dados continua a aumentar e os serviços em cloud estão eles próprios dependentes de terceiros, também eles sujeitos a ciberataques (ver "A indústria do ransomware").

A quantidade total de dados armazenados na nuvem (em serviços de cloud) – desde os obtidos nas clouds públicas ao enorme volume gerado pelos serviços privados nas infra-estruturas das redes sociais (Facebook, TikTok ou X) - poderá atingir os 200 zetabytes (ZBs) em 2025, o equivalente a 50% do total ds dados mundiais gerados nessa data, antecipa a Cybersecurity Ventures.

Um ZB é o equivalente a um bilião de gigabytes, um espaço de armazenamento capaz de albergar mais de 12 milhões de vídeos em resolução 4K. No entanto, uma reportagem recente apontava como "88% do que é armazenado na nuvem é considerado lixo que não será acedido novamente pelos utilizadores".

Por questões legais, entre outras, esse "lixo" deverá manter-se armazenado nas instalações do fornecedor de serviços de cloud ou gerido pelo proprietário dos dados, com custos inerentes ao seu processamento computacional e manutenção energética.

Esta última será uma preocupação constan-

are also subject to cyberattacks (see 'The ransomware industry').

The total amount of cloud-stored data (in cloud services) - from that obtained in public clouds to the enormous volume generated by private services in social media infrastructures (Facebook, TikTok or X) - could reach 200 zetabytes (ZBs) by 2025, equivalent to 50 % of the world's total data generated by then, predicts Cybersecurity Ventures.

1 ZB is equivalent to 1 billion gigabytes, a storage space capable of holding more than 12 million videos in 4K resolution. However, a recent report pointed out that '88 % of what is stored in the cloud is considered junk data that will not be accessed again by users.'

For legal reasons, among others, this 'junk' must remain stored on the premises of the cloud service provider or managed by the data owner, with costs inherent in its computer processing and energy maintenance.

The latter will be a constant concern in the coming years, with a natural financial impact on the management of data centres.

For Elon Musk, 'the next shortage will be electricity. They won't be able to find enough electricity to run all the chips. I think [in 2025], you'll see they just can't find enough electricity to run all the chips,' not least because of the 'simultaneous

Fonte: DOMO

te nos próximos anos, com natural impacto financeiro na gestão dos centros de dados.

Para Elon Musk, "a próxima escassez será de eletricidade. Não se vai conseguir ter eletricidade suficiente para fazer funcionar todos os processadores. Penso que [em 2025] veremos que não se consegue ter eletricidade su-

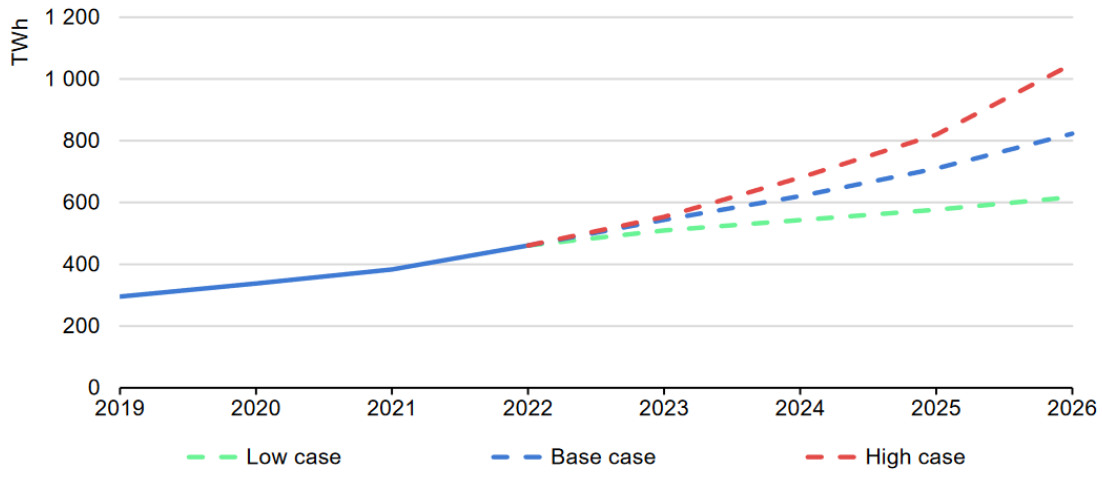
growth of electric cars and AI, both of which need electricity, both of which need voltage transformers - I think, is creating a tremendous demand for electrical equipment and for electrical power generation.'

The International Energy Agency (IEA) looks at other sectors with growing electricity

ficiente para fazer funcionar todos os 'chips'", até pelo "crescimento simultâneo dos carros elétricos e da IA, ambos necessitando de eletricidade, ambos necessitando de transformadores de tensão - penso que se está a criar uma enorme procura de equipamento elétrico e de produção de energia elétrica".

consumption and anticipates, in its Electricity 2024 report, that 'global electricity demand is expected to rise at a faster rate over the next three years, growing by an average of 3.4 % annually through 2026', largely due to the electrification of the residential and transport sectors and 'a notable expansion

Global electricity demand from data centres, AI, and cryptocurrencies, 2019-2026



IEA. CC BY 4.0.

A International Energy Agency (IEA) olha para outros setores com crescente consumo elétrico e antecipa, no relatório Electricity 2024, que "a procura mundial de eletricidade aumente a um ritmo mais rápido nos próximos três anos, crescendo em média 3,4% ao ano até 2026", muito devido à eletrificação dos setores residencial, dos transportes e "por uma expansão notável do setor dos centros de dados". Para a IEA, o consumo de eletricidade destes centros, da inteligência artificial (IA) e do setor das

of the data centre sector.' According to the IEA, the electricity consumption from data centres, artificial intelligence (AI) and the cryptocurrency sector 'could double by 2026. Data centres are significant drivers of growth in electricity demand in many regions. After globally consuming an estimated 460 terawatt-hours (TWh) in 2022, data centres' total electricity consumption could reach more than 1 000 TWh in 2026.'

Also according to the IEA, there are more

criptomoedas "poderá duplicar até 2026. Os centros de dados são motores significativos do crescimento da procura de eletricidade em muitas regiões. Depois de consumir globalmente cerca de 460 terawatts-hora (TWh) em 2022, o consumo total de eletricidade dos centros de dados poderá atingir mais de 1.000 TWh em 2026".

Ainda segundo a IEA, existem mais de 8.000 centros de dados a nível mundial, com 33% localizados nos EUA, seguidos por 16% na Europa (1.240 instalações em 2022, com um consumo abaixo dos 100 TWh em 2022, com a maioria concentrada junto dos principais centros financeiros (Frankfurt, Londres, Amesterdão, Paris ou 82 na Irlanda, neste caso pelas benesses fiscais).

Portugal, pelas contas do Data Center Map, terá 33 destas instalações, principalmente localizadas na região de Lisboa (17) e uma dezena na zona do Porto, estando as restantes dispersas. O número poderá ser maior, totalizando uns "insuficientes" 38 centros de dados, com mais sete em "pipeline", segundo a análise da Worx Real Estate Consultants de junho passado.

Naturalmente, todo este consumo energético, a ocupação de espaço físico e consequentes impactos ambientais têm requerido alguma atenção e levado à procura de alternativas mais sustentáveis, eficientes e fiáveis.

than 8 000 data centres worldwide, 33 % of them being in the USA, followed by 16 % in Europe (1 240 facilities in 2022, with a consumption of less than 100 TWh in 2022, the majority concentrated near the main financial centres (Frankfurt, London, Amsterdam, Paris or 82 in Ireland, in this case due to tax benefits).

According to the Data Centre Map, Portugal will have 33 of these facilities, mainly located in the Lisbon region (17) and a dozen in the Porto area, with the rest scattered around the country. The number could be higher, with a total 'insufficient' of 38 data centres, with another seven in the pipeline, according to an analysis by Worx Real Estate Consultants last June.

Naturally, all this energy consumption, the occupation of physical space and the consequent environmental impacts have required some attention and led to the search for more sustainable, efficient and reliable alternatives.

The data centre industry 'has embraced more sustainable solutions in recent years, becoming a significant investor in renewable power at the corporate level. According to recent calculations, 'sites that leased wind and solar capacity jumped 50 percent year over year as of early 2023, to more than 40 gigawatts'. Still, 'demand outpaces those investments.' This is why provisional solutions or new technological approaches

Fonte: Google

A indústria dos centros de dados "adotou soluções mais sustentáveis nos últimos anos, tornando-se um investidor significativo em energia renovável ao nível corporativo. Os locais que alugaram capacidade eólica e solar aumentaram 50% ao ano no início de 2023, para mais de 40 gigawatts", segundo cálculos recentes, mas "a procura supera esses investimentos". Por isso, procuram-se soluções provisórias ou novas aproximações tecnológicas, desde o armazenamento em ADN (num "fluxo de informação entre digital e biológico em que todas as preocupações de segurança do mundo das TI serão também introduzidas no mundo da biologia"), à extensão da vida útil dos servidores de cinco para seis anos, ou ao investimento nos centros de dados em hiperescala ("hyperscale data centers"), capazes de executar operações em grande escala sem aumento do consumo elétrico mas que terão necessariamente de revelar novas abordagens mais seguras, como alertou a ENISA.

are being sought, from DNA storage (in a 'this flow of information back and forth between the digital and the biological will mean that every security concern from the world of IT will also be introduced into the world of biology') to extending the lifespan of servers from five to six years, or investing in hyperscale data centres, capable of running large-scale operations without increasing electricity consumption but which will necessarily have to reveal new, more secure approaches, as ENISA warned.

Ciberincidentes lideram riscos de negócio em Portugal

Os ciberincidentes continuam a liderar a lista de potenciais riscos em Portugal, registados no Allianz Risk Barometer no ano passado e agora para 2024. Segue-se a interrupção da continuidade do negócio, desenvolvimentos macroeconómicos (de impacto negativo), catástrofes naturais, crise energética. Na segunda metade da lista, constam as mudanças legislativas e regulatórias, alterações climáticas, escassez de força de trabalho competente, incêndios e desenvolvimentos de mercado, como concorrência intensa ou estagnação do mercado.

Cyber incidents top the list of business risks in Portugal

Cyber incidents continue to top the list of potential risks in Portugal, recorded in the Allianz Risk Barometer for 2023 and now for 2024. It is followed by interruption of business continuity, macroeconomic developments (with a negative impact), natural disasters and the energy crisis. The second half of the list includes legislative and regulatory changes, climate change, shortages of a competent workforce, fires and market developments, such as intense competition or market stagnation.

Top 10 risks in Portugal

Source: Allianz Commercial. Figures represent how often a risk was selected as a percentage of all responses for that country.
Respondents: 33. Figures don't add up to 100% as up to three risks could be selected

Rank		Percent	2023 rank	Trend
1	Cyber incidents *(e.g., cyber crime, IT network and service disruptions, malware / ransomware, data breaches, fines, and penalties)*	48%	*1 (59%)*	→
2	Business interruption *(incl. supply chain disruption)*	36%	*5 (26%)*	↑
3	Macroeconomic developments *(e.g., inflation, deflation, monetary policies, austerity programs)*	30%	*2 (44%)*	↓
3	Natural catastrophes *(e.g., storm, flood, earthquake, wildfire, extreme weather events)*	30%	*4 (28%)*	↑
5	Energy crisis *(e.g., supply shortage / outage, price fluctuations)*	24%	*3 (36%)*	↓
6	Changes in legislation and regulation *(e.g., tariffs, economic sanctions, protectionism, Euro-zone disintegration)*	18%	*9 (10%)*	↑
6	Climate change *(e.g., physical, operational, and financial risks as a result of global warming)*	18%	*7 (13%)*	↑
6	Shortage of skilled workforce	18%	*6 (15%)*	→
9	Fire, explosion	15%	*7 (13%)*	↓
9	Market developments *(e.g., intensified competition / new entrants, M&A, market stagnation, market fluctuation)*	15%	*9 (10%)*	→

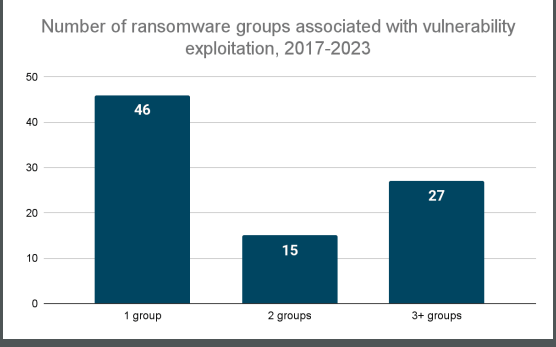
Padrões e alvos de exploração de vulnerabilidades por ransomware (2017-2023)
Patterns and targets for ransomware exploitation of vulnerabilities(2017-2023)

Uma análise recente da Insikt analisou as tendências do ransomware e das vulnerabilidades nos últimos anos, perspetivando as expectativas futuras. Em termos rápidos, os grupos de ransomware exploram vulnerabilidades escolhidas por alguns grupos e as amplamente exploradas por vários grupos, definindo assim estratégias de defesa diferentes.

As últimas vulnerabilidades são mais exploradas no software empresarial mais generalizado, salientando-se a necessidade da sua rápida correção, entre outras. Quanto aos grupos que se concentram na exploração de três ou mais vulnerabilidades, fornecem padrões claros de alvos para os defensores e estão igualmente em software empresarial amplamente utilizado.

A análise nota que "uma potencial recuperação do valor das criptomoedas pode fazer com que os grupos de extorsão se concentrem mais no roubo de carteiras de criptomoedas do que na investigação de vulnerabilidades".

A recent Insikt analysis took a look at ransomware and vulnerability trends over the last few years to offer insights into future expectations. In sum, ransomware groups exploit vulnerabilities chosen by a few groups and those widely exploited by several groups, thus defining different defence strategies.



The latter vulnerabilities are more exploited in more generalised business software, emphasising the need for their rapid correction, among others interventions. As for the groups that focus on exploiting three or more vulnerabilities, these provide clear target patterns for defenders and can also be found in commonly used enterprise software.

The analysis notes that 'a potential rebound in cryptocurrency value might shift extortion groups' focus towards crypto wallet theft from vulnerability research.'

3

Marcos Eckart Esteves

Sénior Manager da Deloitte
Senior Manager at Deloitte

1. Quais as oportunidades existentes para a obtenção de financiamento público dirigido a projetos na área da cibersegurança?

Atualmente, existem várias oportunidades, as quais podem ser subdivididas em dois tipos de programas: os programas europeus, geridos diretamente pela União Europeia, e os programas nacionais.

A nível europeu, destaca-se desde logo o Programa Europa Digital, um programa de financiamento focado em levar a tecnologia digital a empresas, cidadãos e administrações públicas. A cibersegurança corresponde a uma das cinco áreas estratégicas do Programa, de que é exemplo um recente aviso de concurso especificamente destinado a projetos nesta área. Esse aviso pretende apoiar, entre outros, projetos de desenvolvimento e implementação de novas tecnologias de cibersegurança para os Security Operation Centres (SOC), projetos de reforço das capacidades de cibersegurança das Pequenas e Médias Empresas (PME) europeias, ou projetos de implementação de sistemas

1. What opportunities are there for cybersecurity projects to get public funding?

There are currently several opportunities, which can be subdivided into two types of programmes: European programmes, managed directly by the European Union, and Portuguese programmes.

At a European level, the Digital Europe Programme stands out. This funding programme is focused on bringing digital technology to companies, citizens and public administrations. Cybersecurity is one of the Program's five strategic areas, an example of which is a recent call for proposals for projects in this area. This call aims to support, among others, projects to develop and implement new cybersecurity technologies for Security Operation Centers (SOC), projects to strengthen the cybersecurity capabilities of European Small and Medium-sized Enterprises (SMEs), or projects to implement post-quantum cryptography systems. Similar calls can be a relevant source of funding for projects in this area.

Also at European level, it is important to mention Horizon Europe, the framework programme for Research and Innovation (R&I) for 2021-2027, which aims to strengthen Europe's leadership position in the field of research and innovation. This programme includes specific pillars aimed at digital transition and transformation,

pós-criptografia quântica. Concursos semelhantes podem ser uma fonte relevante de financiamento para projetos nesta área.

Ainda a nível europeu, importa mencionar o Horizonte Europa, o programa-quadro de Investigação e Inovação (I&I) para o período de 2021-2027 e que visa reforçar a posição de liderança da Europa no domínio da investigação e inovação. Este programa contém pilares específicos direcionados para a transição e transformação digital, onde o tema da cibersegurança pode ser enquadrado.

Por sua vez, a nível nacional, destaca-se o Programa Portugal 2030, o quadro financeiro plurianual para o período 2021-2027, que conta com regimes específicos de apoio à Investigação e Desenvolvimento (I&D), capacitação digital, qualificação e internacionalização de PME, entre outros, que poderão financiar projetos na área da cibersegurança ou projetos de âmbito mais alargado em que a cibersegurança represente uma componente relevante. Adicionalmente, releva-se o Plano de Recuperação e Resiliência (PRR), que, embora numa fase mais adiantada de execução, apresenta também um conjunto de regimes que poderão financiar projetos neste domínio, em particular na dimensão "Transição Digital", onde a cibersegurança pode desempenhar um papel preponderante.

A acrescer aos regimes de incentivos financeiros supramencionados, poderão ainda existir oportunidades de apoios a nível fiscal (para as empresas), em particular ao nível de deduções à coleta de IRC, sendo de destacar

where the topic of cybersecurity can also be included.

At national level, the Portugal 2030 Programme, the multiannual financial framework for 2021-2027 stands out with specific support schemes for Research and Development (R&D), digital training, and qualification and internationalisation of SMEs, among others. These schemes can be used to fund projects in cybersecurity or projects with a broader scope in which cybersecurity is a relevant component. Additionally, there is also the Recovery and Resilience Plan (PRR), which, although at a more advanced stage of implementation, also has a number of schemes that could fund projects in this area, namely in the area of 'Digital Transition', where cybersecurity can play a major role.

In addition to the abovementioned financial incentive schemes, there may also be opportunities for tax support (for companies), namely in the form of corporate income tax (IRC) deductions. Of particular note in this regard is SIFIDE, the Corporate R&D Tax Incentive Scheme which finances R&D projects in any field (and where cybersecurity can be included), or the Investment Support Tax Scheme, which finances technology transfer expenses, among others.

For the abovementioned support schemes, the co-financing rates range from 25 to 100 % of eligible expenses, depending on the schemes in question, the configuration

a este respeito o Sistema de Incentivos Fiscais em I&D Empresarial (SIFIDE), que financia projetos de I&D em qualquer domínio (e onde a cibersegurança se pode enquadrar), ou o Regime Fiscal de Apoio ao Investimento, que financia, entre outras, despesas de transferência de tecnologia.

Para os regimes de apoio mencionados, as taxas de cofinanciamento estão compreendidas entre 25% a 100% das despesas elegíveis, dependendo dos regimes em causa, da configuração dos projetos e da tipologia das entidades beneficiárias.

2. Em termos de recomendações, quais são as características que as organizações devem precaver nos seus projetos de cibersegurança de forma a preparem uma candidatura robusta?

No momento de preparação de qualquer processo de candidatura a financiamento público, recomenda-se uma análise pormenorizada dos regulamentos aplicáveis e respetivos avisos de abertura de concurso, de forma a compreender as regras, as condições de elegibilidade dos projetos, as obrigações subjacentes à obtenção dos apoios, as tipologias de despesas elegíveis e, bem assim, as condições em que o financiamento é atribuído.

De seguida, importa compreender se o projeto se adequa aos objetivos previstos no regulamento e no aviso, nomeadamente em termos de âmbito, dimensão e escala, período temporal de execução, entre outros.

of the projects and the type of beneficiary entities.

2. In terms of recommendations, what characteristics should organisations look out for in their cybersecurity projects in order to prepare a robust application?

When preparing any application for public funding, we recommend a detailed analysis of the applicable regulations and calls for tenders in order to understand the rules, the eligibility conditions for projects, the obligations involved in obtaining support, the types of eligible expenditure and the conditions under which funding is awarded.

Next, it is important to understand whether the project is in line with the objectives set out in the regulation and the call, namely in terms of scope, size and scale, and timeframe for implementation, among others.

Once these items have been checked, organisations can then proceed with preparing applications. In this process, it is recommended to use clear, concise and direct language, seeking to align the scope and objectives of the project with the goals defined in the regulation and/or call. You should also be able to quantify the project's impact on the organisation, sector, region and/or society in general, where applicable.

In the specific case of applications to European funding programmes, it is also

Uma vez validados estes pontos, as entidades poderão, então, avançar com o processo de preparação das candidaturas. Neste processo, recomenda-se utilizar uma linguagem clara, concisa e direta, procurando alinhar o âmbito e objetivos do projeto com as metas definidas no regulamento e/ou aviso. Deve-se igualmente conseguir estimar, de forma quantificada, os impactos do projeto para a organização, setor, região e/ou sociedade em geral, sempre que aplicável.

No caso específico de candidaturas a programas de financiamento europeu, é ainda recomendável entrar em contacto com os pontos de contacto nacionais de cada programa (estes pontos de contacto encontram-se normalmente identificados nos sítios *web* dos programas de financiamento respetivos, sendo de destacar, em Portugal, na área da cibersegurança, a Agência Nacional de Inovação ou o Centro Nacional de Cibersegurança). Os pontos de contacto nacionais podem prestar aconselhamento quanto ao eventual enquadramento do projeto no aviso de concurso identificado, ajudar a encontrar sinergias com outros programas e/ou entidades, ou inclusive ajudar a encontrar e/ou formar consórcios, de modo a robustecer e enriquecer os projetos.

3. Para além da obtenção de financiamento para os seus projetos, que outras vantagens existem na preparação e gestão de candidaturas a financiamento público na área da cibersegurança?

advisable to get in touch with the national contact points for each programme (these contact points are usually identified on the websites of the corresponding funding programmes; in Portugal, in the area of cybersecurity, the Agência Nacional de Inovação [National Innovation Agency] or the Centro Nacional de Cibersegurança [Portuguese National Cybersecurity Centre] stand out).

The national contact points can advise applicants on whether the project fits into the call for proposals identified, help find synergies with other programmes and/or entities, or even help find and/or form consortia in order to strengthen and enrich the projects.

3. Apart from obtaining funding for your projects, what other advantages are there in preparing and managing applications for public funding in the area of cybersecurity?

My experience in monitoring and managing projects tells me that applications for public funding help to better structure investments and discipline teams to achieve measurable, high-value results for organisations. As a rule, these application processes also require the definition of timeframes and detailed work plans, with targets and deliverables, which, in my opinion, are an asset for the successful execution of projects.

On the other hand, this generates a greater

A minha experiência no acompanhamento e gestão de projetos diz-me que as candidaturas a financiamento público ajudam a estruturar melhor os investimentos e a disciplinar as equipas para o alcance de resultados mensuráveis de elevado valor para as organizações. Normalmente, estes processos de candidatura obrigam, ainda, à definição de cronogramas e planos de trabalho detalhados, com metas e entregáveis, o que, a meu ver, se revela uma mais-valia para uma execução bem-sucedida dos projetos.

Por outro lado, gera-se um maior comprometimento das organizações com os objetivos definidos em candidatura e assiste-se a ganhos de conhecimento e de experiência por parte das equipas envolvidas, que podem catapultar as entidades beneficiárias para níveis superiores de organização/oferta.

Adicionalmente, este tipo de projetos, se desenvolvidos em consórcio, promovem o estabelecimento de parcerias e sinergias na cadeia de valor, o que permite partilha de experiências e de conhecimento, clientes e mercados, ajudando ao crescimento sustentado das organizações em ecossistemas vivos.

Por último, importa referir que muitos destes programas de financiamento premeiam, com taxas de financiamento mais elevadas, os projetos que englobem um plano de partilha e disseminação de conhecimento, o que, na área específica da cibersegurança, pode representar uma vantagem acrescida para o setor.

commitment on the part of organisations to the objectives defined in the application. The teams involved acquire new insights and experience, which can catapult the beneficiary organisations to higher levels of organisation/offering.

In addition, when these types of projects are developed in consortia, they promote the creation of partnerships and synergies in the value chain, which allows for the sharing of experiences and knowledge, clients and markets, helping the sustained growth of organisations in living ecosystems.

Lastly, it should be noted that many of these funding programmes reward projects that include a knowledge sharing and dissemination plan with higher funding rates, which, in the specific area of cybersecurity, can be an added advantage for the sector.

Vasco Sampaio

Consultor de comunicação, Hill & Knowlton Portugal
Communications Consultant, Hill & Knowlton Portugal

Ciberataques e comunicação segura

Os ciberataques são, hoje, algumas das principais ameaças que uma empresa ou organização pode enfrentar. Num momento em que a informação é cada vez mais imediata e multicanal, neste tipo de crises, como em qualquer outro, é esperada das organizações uma resposta rápida e esclarecedora em todas as frentes. Sem esta comunicação, a crise de segurança pode afetar não apenas a operação, mas também a reputação e continuidade do negócio.

Impõe-se, por isso, uma reação de duas formas: resolvendo não só o problema e garantindo a segurança da sua operação, mas também trabalhando na forma como clientes e parceiros olham para esse problema e como a empresa o ataca e tenta ultrapassar. Como diz o provérbio, à mulher de César não basta ser, deve parecer. E para uma empresa vencer de facto uma crise, tem de comunicar e de convencer o seu público de que a superou.

As crises, independentemente da origem ou tipologia, têm vários aspetos em comum: o fator surpresa, a falta de tempo para responder, a falta de recursos, perda de con-

Cyberattacks and safe communications

Nowadays, cyberattacks are some of the main threats a company or organisation can face. At a time when information is increasingly immediate and multichannel, in this type of crisis, as in any other, organisations are expected to respond quickly and with clarity on all fronts. Without this communication, a security crisis can affect not only the operation, but also a business' reputation and its continuity.

It is thus necessary to react in two ways: not only by resolving the problem and guaranteeing the security of operations, but also by working on the way clients and partners look at this problem and how the company tackles it and tries to overcome it. As the saying goes, it is not enough for Caesar's wife to be virtuous, she must be seen to be virtuous. And for a company to really overcome a crisis, it has to communicate and convince its public that it has actually overcome it.

Regardless of their origin or type, crises have several aspects in common: the surprise factor, lack of time to respond, lack of resources, perceived or real loss of control, and an escalation of events that jeopardise

trolo percecionada ou real, e um escalar de acontecimentos que prejudicam os processos normais de tomada de decisão. Gerir uma crise de comunicação, tal como gerir uma crise de cibersegurança, exige uma tomada de decisões ágil e coordenada, parte de uma estratégia clara, integrada e com um objetivo-chave: o de minimizar danos às operações, ao desempenho e à reputação da empresa.

Preparação

O primeiro e mais importante ponto é a preparação, para assegurar que a empresa conhece os riscos, tem um sistema de identificação de alertas, tem traçados os cenários e prepara, antecipadamente, diferentes tipos de resposta e ferramentas de comunicação. A preparação ajuda a assegurar previsibilidade, consistência, maior margem de manobra e tempo para a tomada de decisão, aspetos raros em qualquer crise. Mas certo é, também, que esta preparação não está ao alcance de todas as empresas e organizações. Saltando este primeiro passo, resta atacar os restantes.

Resposta

Com ou sem preparação, qualquer crise exige uma resposta: resolver ou corrigir a situação que levou à crise, garantindo que os impactos do ciberataque, por exemplo, são cuidadosamente medidos e devidamente conhecidos. Uma resposta só é eficaz se não deixar pontas soltas, que vão certamente

normal decision-making processes. Managing a communications crisis, just like managing a cybersecurity crisis, requires agile and coordinated decision-making as part of a clear, integrated strategy with a key objective: to minimise damage to the company's operations, performance and reputation.

Preparation

The first and most important point is preparation, to ensure that a company knows the risks, has a system for identifying alerts, has outlined the scenarios and prepares different types of response and communication tools in advance. Preparation helps to ensure predictability, consistency, greater room for manoeuvre and time for decision-making, all of which are rare during any crisis. But it is also true that this preparation is not available to all companies and organisations. Having skipped this first step, all that remains is to tackle the other ones.

Response

With or without preparation, any crisis requires a response: resolving or correcting the situation that led to the crisis, ensuring that the impacts of the cyberattack, for example, are carefully measured and properly known. A response is only effective if it leaves no loose ends, which will certainly multiply the impact of the crisis and the possible damage to the company's reputation. With

multiplicar o impacto da crise e os possíveis danos à reputação da empresa. Com este momento chega a primeira oportunidade de comunicação: a de assumir responsabilidades, lamentar e explicar, de forma transparente, o que aconteceu, porque aconteceu, como afetou a empresa, que impacto teve nos clientes e parceiros e que impacto pode ainda vir a ter; e a de dar segurança a todos os afetados, delimitando claramente o que foi afetado e traçando o caminho a percorrer, desse momento em diante, para resolver os problemas e continuar a operação.

Resolução

Neutralizada a ameaça e corrigidas as causas iniciais da crise, é fundamental um momento de avaliação de resultados, de análise da estratégia escolhida e de deteção de áreas a melhorar, lições a reter e alterações a aplicar. Numa crise de comunicação, esta é uma segunda oportunidade para reforçar as mudanças que foram realizadas, e que darão reforçada confiança a clientes e parceiros. No fim da tempestade, quem lida diretamente com a empresa ou organização tem de saber porque deve continuar a trabalhar com ela. Aí, a honestidade e clareza com que uma entidade lida com este tipo de situações é um selo de segurança e confiança para o futuro.

Tomar controlo

Uma crise é um momento de aflição, pressa e nervosismo. Mas é também de humildade, determinação e liderança. Uma resposta efi-

this moment comes the first opportunity for communication: taking responsibility, expressing regret and explaining, in a transparent way, what happened, why it happened, how it affected the company, what impact it had on clients and partners and what impact it may still have; and providing reassurance to all those affected, clearly delineating what was affected and outlining the path to be followed, from that moment on, to resolve the problems and resume operations.

Resolution

Once the threat has been neutralised and the initial causes of the crisis have been corrected, it is essential to assess the results, analyse the chosen strategy and detect areas for improvement, lessons to be retained and changes to be made. In a communication crisis, this is a second opportunity to reinforce the changes that have been made, which will give clients and partners greater confidence. At the end of the storm, those who deal directly with the company or organisation need to know why they should continue to work with it. There, the honesty and clarity with which an organisation deals with this type of situation is a seal of security and trust for the future.

Taking control

A crisis is a time of distress, haste and nervousness. But it is also a time for humility, determination and leadership. An effective

caz a uma crise de comunicação passa por uma comunicação inequívoca por parte da instituição afetada: deve ser ela a contar a sua própria história, a defini-la nos seus próprios termos e a apresentar claramente a sua narrativa, de forma a evitar especulação e a corrigir mal-entendidos. Um bom porta-voz não se esconde e percebe as dúvidas, a curiosidade e a preocupação dos clientes, do público e dos jornalistas. Recebe perguntas com humildade, contextualiza as respostas e não hesita em esclarecer diretamente. Se uma organização não contar a sua história, outros a contarão. Uma comunicação proativa, e não reativa, dá maior segurança ao público, limita os danos sofridos pela organização e ajuda a passar a mensagem de que a empresa será capaz de fazer o caminho que tem pela frente.

Segurança é a palavra-chave, não apenas quando o tema são os ciberataques. Segurança é o que a empresa ou instituição deve priorizar e proteger, mas também o que deve cultivar, na sua audiência, nos momentos mais difíceis. As crises têm a vantagem e desvantagem de atrair atenções: são momentos de aperto, alta pressão e muito nervosismo, mas são também palcos e tempos de antena para a definição de uma narrativa e mensagem claras. Uma crise grave vai sempre marcar a empresa e a sua imagem, mas uma resposta inequívoca, que mostre liderança, vai projetá-la como uma organização honesta, fiável e convidativa, com a qual qualquer cliente ou parceiro quererá trabalhar.

response to a communication crisis involves an unequivocal communication on the part of the affected institution: it must tell its own story, define it in its own terms and clearly present its narrative in order to avoid speculation and correct misunderstandings. A good spokesperson does not hide and understands the doubts raised, curiosity and concerns of clients, the public and journalists. They welcome questions with humility, contextualise the answers and do not hesitate to clarify directly. If an organisation does not tell its story, others will. A proactive communication, rather than a reactive one, gives the public greater security, limits the damage sustained by the organisation and helps convey the message that the company will be able to continue the journey ahead.

Security is the key word, not just when it comes to cyberattacks. Security is what the company or institution must prioritise and protect, but also what it must cultivate in its audience during the most difficult times. Crises have the advantage and disadvantage of attracting attention: they are moments of distress, high pressure and a lot of nervousness, but they are also stages and opportunities for defining a clear narrative and message. A serious crisis will always leave its mark on a company and its image, but an unequivocal response that shows leadership will project it as an honest, reliable and inviting organisation that any client or partner will want to work with.

PTSOC analisa acontecimentos e tendências do ano do ransomware

O PTSOC publicou o seu Relatório Anual relativo a 2023, em que apresenta uma súmula de acontecimentos e tendências relativas aos domínios da cibersegurança no ano passado "e colocar em perspetiva os principais desafios que se antecipam para 2024".

PTSOC analyses events and trends in the year of ransomware

PTSOC has published its Annual Report for 2023, in which it summarises the events and trends in cybersecurity over the past year 'and puts into perspective the main challenges that lie ahead for 2024.'

Quanto custam os ciberataques?

O custo dos ciberataques pode ter atingido os 8.000 biliões de dólares em 2023, valor que deve aumentar para os 9.500 biliões este ano e continuar a crescer para os 10.500 biliões em 2025. Um ciberataque médio atinge os 4.450 milhões de dólares, com o setor dos cuidados de saúde a registar as perdas médias mais elevadas.

Quanto a países, os EUA lideram em perdas (média anual de 9.480 milhões de dólares), seguidos pelo Médio Oriente com um pouco mais de oito mil milhões de dólares por ano.

YEAR	ESTIMATED ANNUAL COST OF CYBER-ATTACKS GLOBALLY (USD)
2024	$9.5 trillion*
2025	$10.5 trillion*
2026	$11.3 trillion**
2027	$12.4 trillion**
2028	$13.8 trillion**
2029	$15.6 trillion^
2030	$17.9. trillion^

*Sources: *Cybersecurity Ventures **Statista ^Our own projections*

How much do cyberattacks cost?

The cost of cyberattacks may have reached 8 trillion USD in 2023, a number that is expected to rise to 9.5 trillion in 2024 and continue to grow to 10.5 trillion in 2025. An average cyberattack reaches losses of 4.45 million USD, with the healthcare industry recording the highest average losses.

In terms of countries, the USA leads the way in losses (annual average of 9.48 million USD), followed by the Middle East with just over 8 million USD yearly.

Cultura de cibersegurança nas organizações
Cyber security culture in organisations

"O conceito de cultura de cibersegurança (CSC) refere-se ao conhecimento, crenças, percepções, atitudes, pressupostos, normas e valores das pessoas relativamente à cibersegurança e à forma como se manifestam no comportamento das pessoas com as tecnologias da informação. A CSC engloba tópicos familiares, incluindo a sensibilização para a cibersegurança e as estruturas de segurança da informação, mas é mais ampla tanto no âmbito como na aplicação, preocupando-se em tornar as considerações de segurança da informação uma parte integrante do trabalho, hábitos e conduta de um funcionário, incorporando-as nas suas ações diárias".

'The concept of Cybersecurity Culture (CSC) refers to the knowledge, beliefs, perceptions, attitudes, assumptions, norms and values of people regarding cybersecurity and how they manifest themselves in people's behaviour with information technologies. CSC encompasses familiar topics including cybersecurity awareness and information security frameworks but is broader in both scope and application, being concerned with making information security considerations an integral part of an employee's job, habits and conduct, embedding them in their day-to-day actions.'

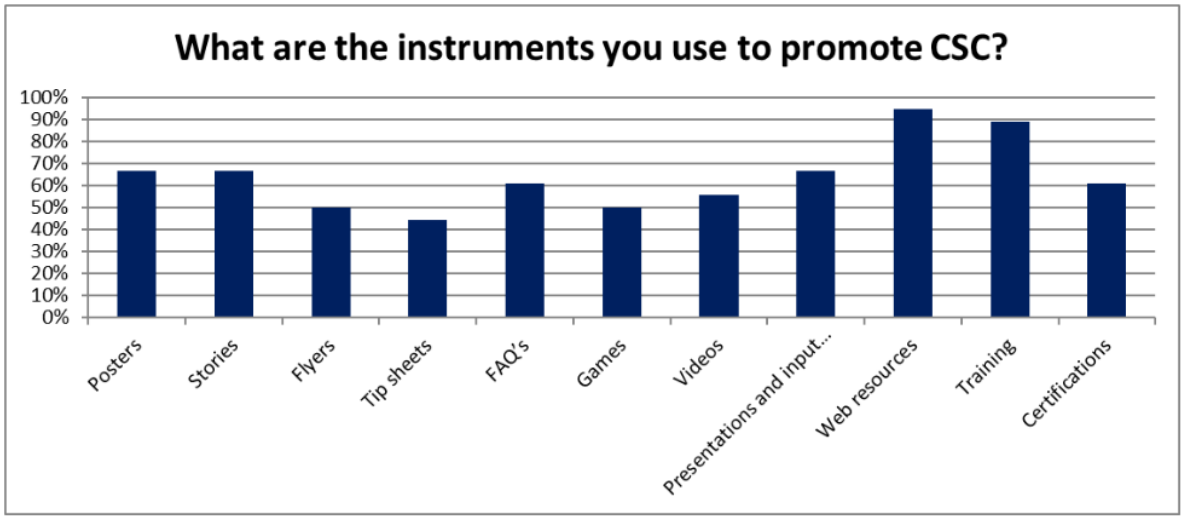


Figure 5: CSC intervention delivery methods

Diretora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design Gráfico | Graphic Design
Sara Dias
Maria Cristóvão

Tradução | Translation
Sara Pereira

Fotografia | Photography
Capa/Cover: Tobias Reich/Unsplash
Índice/Index: Imagem gerada em IA

Publicação trimestral | Quarterly publication
Abril 2024 | April 2024