bilingual edition

ptsoc {news}

A cibersegurança da cadeia de fornecimento

3 perguntas a Luisa Ribeiro Lopes

Os desafios dos Planos de Continuidade de Negócio e das Soluções de Disaster Recovery em particular por Filipe Frasquilho

18

The cybersecurity of the supply chain

3 questions to Luisa Ribeiro Lopes

The challenges of Business Continuity Plans and Disaster Recovery Solutions in particular by Filipe Frasquilho

.pt

A cibersegurança da cadeia de fornecimento

A 20 de Maio passado, cibercriminosos roubaram terabytes de dados pessoais do serviço de venda eletrónica de bilhetes para eventos ao vivo Ticketmaster, colocando-os **à venda online**. Também o banco Santander no Chile, Espanha, **EUA** e Uruguai sofreu acessos ilegítimos a "contas bancárias de 30 milhões de clientes", **segundo os criminosos**. O mesmo sucedeu a mais de 160 entidades. Em comum, todas eram clientes da empresa de cloud Snowflake, que **rejeitou** ter sofrido qualquer ataque desta amplitude à sua rede.

Os criminosos, denominados ShinyHunters, revelaram mais tarde terem acedido a vários fornecedores com ligações às contas da Snowflake, em particular um funcionário da EPAM Systems, empresa de software da Bielorrússia parceira da Snowflake. A Mandiant **confirmou** o acesso ilegal à empresa de cloud através de credenciais comprometidas de clientes mas, para a EPAM, tudo não passou de uma invenção dos atacantes. A revista Wired considera possível que os ShinyHunters "não tenham pirateado diretamente o trabalhador da EPAM e tenham simplesmente obtido acesso às contas da Snowflake usando nomes de utilizador e palavras-passe que obtiveram de antigos repositórios de credenciais roubadas".

Esta intrincada ligação entre vítimas de um

The cybersecurity of the supply chain

On 20 May, cybercriminals stole terabytes of personal data from Ticketmaster, the digital ticketing service for live events, putting them up **for sale online**. Santander bank in Chile, Spain, the **USA** and Uruguay also suffered illegitimate access to 'the bank accounts of 30 million customers', **according to the criminals**. The same happened to more than 160 other organisations. In common, they were all clients of the cloud company Snowflake, which has **denied** having suffered any attack of this scale on its network.

The criminals, referred to as ShinyHunters, later disclosed they had accessed several suppliers with links to Snowflake accounts, namely an employee of EPAM Systems, a Belarusian software company that is a partner of Snowflake. Mandiant **confirmed** illegal access to the cloud company via compromised customer credentials; for EPAM, however, it was all just an invention by the attackers. Wired magazine considers it possible that the ShinyHunters 'did not directly access the EPAM worker and simply gained access to Snowflake accounts using usernames and passwords they obtained from old repositories of stolen credentials'.

This intricate link between victims of an attack with the same origin has been reproduced, affecting small and large organisations alike, as long as there is a single connection (**even**

ataque com a mesma origem tem-se reproduzido e afeta pequenas e grandes organizações, desde que exista um ponto de ligação (mesmo que indireto), afetando os pacientes de hospitais em Londres ou funcionários de uma consultora.

Os elos mais fracos

Estes episódios, pela grande magnitude dos números de dados acedidos, destacam os diferentes riscos na cibersegurança de empresas terceirizadas (em "outsourcing") e a gestão da cadeia de fornecimento ou abastecimento ("management supply chain").

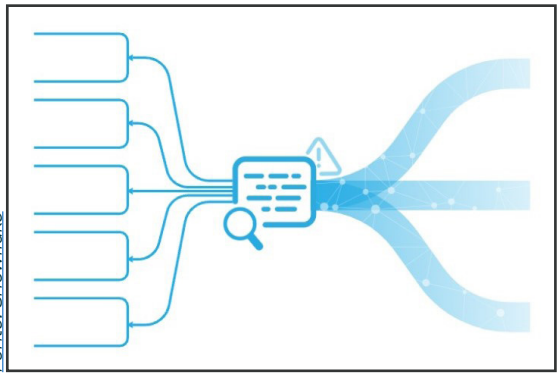
A expressão foi inicialmente usada numa entrevista em 1982 por Keith Oliver, consultor da Booz Allen Hamilton, e definia "o processo de planeamento, implementação e controlo das operações da cadeia de abastecimento com o objetivo de satisfazer as necessidades dos clientes da forma mais eficiente possível. Abrange todo o movimento e armazenamento de matérias-primas, inventário de trabalho em processo e produtos acabados desde o ponto de origem até ao ponto de consumo".

A globalização e a digitalização aceleraram a adoção do modelo na década de 1990, até se atingir um exagerado nível de dependência, como ficou demonstrado durante a crise epidémica do COVID-19.

O elevado grau de interdependências potencia naturalmente a existência de elos fracos

if indirect), affecting patients in London hospitals or employees of a consultancy.

The weakest links



Fonte: Snowflake

Due to the sheer magnitude of the numbers of data accessed, these episodes highlight the different risks in the cybersecurity of outsourcing companies and management supply chain.

The expression was first used in an interview in 1982 by Keith Oliver, a consultant at Booz Allen Hamilton, and it defined 'the process of planning, implementing and controlling the operations of the supply chain with the purpose to satisfy customer requirements as efficiently as possible. It spans all movement and storage of raw materials, work-in-process inventory and finished goods from point-of-origin to point-of-consumption.'

Globalisation and digitalisation have accelerated the adoption of the model in the 1990s, until it reached an exaggerated level of dependency, as shown during the COVID-

O porquê dos ataques à "supply chain"

62% do mercado dos produtos e serviços tecnológicos está nas mãos de apenas 15 empresas. Esta enorme concentração representa uma grande fragilidade para toda a economia global, quando os ciberatacantes têm um interesse acrescido na explosão dos vetores de ataque da cadeia de abastecimento por duas razões:

1. Operações em grande escala. Ao comprometer uma organização, também ganham acesso aos seus clientes - que podem ser centenas ou milhares.

2. Contornar ou iludir as defesas de segurança dos clientes. Um programa de cibersegurança de mil milhões de dólares de uma empresa é tão bom como um do seu fornecedor mais pequeno.

Why are supply chain attacks happening

62 % of the market for technological products and services is in the hands of just 15 companies. This enormous concentration represents a major weakness for the entire global economy, when cyber attackers have an increased interest in exploding supply chain attack vectors for two reasons:

1. Large-scale operations. By compromising an organisation, they also gain access to its customers - who can reach hundreds or thousands.

2. Bypassing or evading customers' security defences. One company's billion-dollar cyber-security programme is just as good as that of its smaller supplier.

Fonte: 2024 Redefining Resilience: Concentrated Cyber Risk in a Global Economy Research

nas cadeias de fornecimento de serviços de software, por exemplo, e são um manancial para cibercriminosos comprometerem dispositivos de um único fornecedor com acesso às contas de vários clientes, colocando estes em significativo risco.

Daí deriva a importância da cibersegurança na cadeia de elementos presentes numa "supply chain", porque não basta assegurar a mesma num elemento da cadeia se existirem falhas noutros. O "efeito dominó" acabará por afetar muitos dos envolvidos. Em sentido inverso, uma boa gestão dos intervenientes tenderá a aumentar a segurança em geral.

Os principais perigos na cadeia de fornecimento são os generalizados na sociedade, desde vulnerabilidades em software de terceiros ao malware e ransomware, ataques

19 epidemic crisis.

The high degree of interdependence naturally leads to weak links in the supply chains of software services, for example, and is seen as a source for cybercriminals to compromise the devices of a single supplier with access to the accounts of several customers, putting them at significant risk.

Hence the importance of cybersecurity in the chain of elements present in a supply chain; it is not enough to ensure it in one element of the chain if there are flaws in others. The domino effect will end up affecting many of those involved. Conversely, good management of those involved will tend to increase security in general.

The main dangers in the supply chain are

de DDoS, phishing ou engenharia social. Esta entrecruza-se com as ameaças internas em qualquer organização, que podem comprometer dados confidenciais e propriedade intelectual, gerar danos financeiros diretos e reputacionais. Pode ainda envolver consequências legais por parte das vítimas e por falhas no cumprimento regulatório, como o Regulamento Geral sobre a Proteção de Dados (RGPD), outras regulamentações sobre dados pessoais e até a conformidade com normas ISO. Também a NIS 2, em fase de transposição nacional, dá uma grande importância à cibersegurança nas cadeias de fornecimento.

No **relatório anual**, o PTSOC antecipou "o advento dos ataques através de supply chain" e explicou como estes "ocorrem quando os atacantes se infiltram nos sistemas por meio de um parceiro ou fornecedor de serviços com acessos privilegiados às redes do alvo. Este será um dos principais vetores de ataque que se perspetiva para 2024, sendo um dos temas a ter de ser endereçado pelas organizações essenciais com a entrada em vigor de diplomas como a NIS 2".

Obrigações regulatórias com efeitos

A **diretiva NIS 2**, em fase de transposição nacional, nota como as pequenas e médias empresas (PMEs) se estão a tornar "cada vez mais alvo de ataques nas cadeias de abastecimento devido às suas medidas menos rigorosas de gestão dos riscos de cibersegurança

those that are widespread in society, from vulnerabilities in third-party software to malware and ransomware, DDoS attacks, phishing or social engineering. This intertwines with internal threats in any organisation, which can compromise confidential data and intellectual property, creating direct financial and reputational damage. It can also have legal consequences for victims and for failures in regulatory compliance, such as the General Data Protection Regulation (GDPR), other regulations on personal data and even compliance with ISO standards. The NIS 2, currently undergoing national transposition, also places great importance on cybersecurity in supply chains.

In its **annual report**, PTSOC anticipated 'the advent of attacks through the supply chain' and explained how they 'occur when attackers infiltrate in systems through a partner or service provider with privileged access to the target's networks. This will be one of the main attack vectors expected for 2024, being one of the topics that will have to be addressed by essential organisations with the entry into force of directives such as NIS 2.

Regulatory obligations with effects

The **NIS 2 directive**, currently undergoing national transposition, notes how small- and medium-sized enterprises (SMEs) are becoming 'increasingly targeted by attacks through the supply chains due to their less

ATTACK TECHNIQUES USED TO COMPROMISE A SUPPLY CHAIN		
	**Malware Infection**	e.g. spyware used to steal credentials from employees.
	**Social Engineering**	e.g. phishing, fake applications, typo-squatting, Wi-Fi impersonation, convincing the supplier to do something.
	**Brute-Force Attack**	e.g. guessing an SSH password, guessing a web login.
	**Exploiting Software Vulnerability**	e.g. SQL injection or buffer overflow exploit in an application.
	**Exploiting Configuration Vulnerability**	e.g. taking advantage of a configuration problem.
	**Physical Attack or Modification**	e.g. modify hardware, physical intrusion.
	**Open-Source Intelligence (OSINT)**	e.g. search online for credentials, API keys, usernames.
	**Counterfeiting**	e.g. imitation of USB with malicious purposes.

Fonte: ENISA

As ameaças vistas pela ENISA

No relatório "Threat Landscape for Supply Chain Attacks", a ENISA nota como, dos 24 ataques a cadeias de abastecimento entre janeiro de 2020 e julho de 2021, cerca de metade foram atribuídos a grupos conhecidos pela comunidade de segurança, cerca de 62% dos ataques aproveitaram-se da confiança dos clientes no fornecedor e, na mesma percentagem, foi usado o malware como técnica de ataque.

Em 66% dos incidentes, "os atacantes focaram-se no código dos fornecedores para comprometer ainda mais os clientes visados" e "cerca de 58% dos ataques à cadeia de abastecimento visavam obter acesso a dados (predominantemente de clientes, incluindo dados pessoais e propriedade intelectual) e cerca de 16% para obter acesso a pessoas".

Threats seen by ENISA

In the 'Threat Landscape for Supply Chain Attacks' report, ENISA notes how, of the 24 attacks on supply chains between January 2020 and July 2021, around half were attributed to groups known to the security community, around 62 % of the attacks took advantage of customers' trust in the supplier and, in the same percentage, malware was used as an attack technique.

In 66 % of incidents, 'attackers focused on supplier code to further compromise targeted customers' and 'around 58 % of supply chain attacks were aimed at gaining access to data (predominantly customer data, including personal data and intellectual property) and around 16 % to gain access to people.'

e de gestão de ataques, bem como ao facto de terem recursos de segurança limitados". Esses ataques têm impacto nas suas operações, "como também podem ter um efeito em cascata em ataques de maior dimensão contra entidades das quais são fornecedoras". Por isso, no âmbito das suas estratégias de cibersegurança, os países devem ajudar as PMEs com um ponto de contacto para orientação e assistência na cibersegurança.

O documento considera "particularmente importante gerir os riscos decorrentes da cadeia de abastecimento de uma entidade e da relação desta com os seus fornecedores, como os prestadores de serviços de armazenamento e tratamento de dados ou os prestadores de serviços de segurança geridos e os editores de software". Relativamente às entidades essenciais, estas devem avaliar "a qualidade e a resiliência globais dos produtos e serviços, as medidas de gestão dos riscos de cibersegurança neles integradas e as práticas de cibersegurança dos seus fornecedores e prestadores de serviços, incluindo os respetivos procedimentos de desenvolvimento seguro", sendo "incentivadas a incorporar medidas de gestão dos riscos de cibersegurança nos acordos contratuais com os seus fornecedores e prestadores de serviços diretos".

Ainda no panorama europeu, o **Digital Operational Resilience Act** (DORA) entrou em vigor em janeiro de 2023 e será aplicável a partir de 2025. Procura reforçar a segurança infor-

stringent cybersecurity risk management and attack management measures, as well as the fact that they have limited security resources.' These attacks have an impact on their operations, 'as well as a cascading effect on larger attacks against organisations of which they are suppliers.' Therefore, as part of their cybersecurity strategies, countries should help SMEs with a point of contact for guidance and assistance in cybersecurity.

The document considers that 'addressing risks stemming from an entity's supply chain and its relationship with its suppliers, such as providers of data storage and processing services or managed security service providers and software editors, is particularly important. Regarding essential organisations, they should assess 'the overall quality and resilience of products and services, the cybersecurity risk-management measures embedded in them, and the cybersecurity practices of their suppliers and service providers, including their secure development procedures', and should be 'encouraged to incorporate cybersecurity risk-management measures into contractual arrangements with their direct suppliers and service providers.'

Also on the European scene, the **Digital Operational Resilience Act** (DORA) came into force in January 2023 and will apply from 2025. It seeks to strengthen the IT security and digital operational resilience of financial organisations (banks, insurance

mática e a resiliência operacional digital das entidades financeiras (bancos, companhias de seguros, empresas de investimento ou de criptomoedas), bem como os seus prestadores externos de serviços TIC. Quando recorrem ao "outsourcing", essas entidades "devem avaliar se e de que forma cadeias de subcontratação potencialmente longas ou complexas podem afetar a sua capacidade de controlar plenamente as funções contratadas".

Com o dever de comunicação de incidentes às autoridades competentes, as entidades financeiras vão ter de lidar com a sua reputação, estando obrigadas a ter um plano de comunicação de crises para a divulgação "dos principais incidentes ou vulnerabilidades relacionadas com as TIC aos clientes e contrapartes, bem como ao público". As referidas autoridades devem publicitar, "sem demora injustificada, qualquer decisão que imponha uma sanção administrativa da qual não caiba recurso".

Nos EUA, o panorama regulatório também se alterou nos meses mais recentes, obrigando as empresas e os seus responsáveis tecnológicos a divulgarem as falhas na gestão da cibersegurança, sob pena de serem acusados judicialmente. "Os CISO encontram-se numa posição delicada: se por um lado os investidores ficam desencorajados por uma postura de ciber-risco deficiente, por outro lado, a SEC será severa com relatórios incorretos. De qualquer forma, os CISO vão estar no centro das atenções", **afirmou** o responsável de

companies, investment or cryptocurrency companies), as well as their external ICT service providers. When outsourcing, these organisations should 'assess whether and how potentially long or complex chains of subcontracting may impact their ability to fully monitor the contracted functions.'

With the duty to report incidents to the competent authorities, financial entities will have to deal with their reputation, and are obliged to have a crisis communication plan for publicising 'major ICT-related incidents or vulnerabilities to clients and counterparties, as well as to the public.' These authorities must publicise, 'without undue delay, any decision imposing an administrative sanction against which there can be no appeal'.

In the USA, the regulatory landscape has also changed in recent months, forcing companies and their CTO to disclose flaws in cybersecurity management, under penalty of prosecution. 'CISOs are in a delicate position: while investors will be put off by a poor cyber risk posture, the SEC will come down hard on inaccurate reports. Either way, CISOs will be in the firing line,' **said** the head of a cybersecurity company.

Different and not always the same

The strategies and technologies for protecting a supply chain are somewhat similar to what each organisation must define for itself. Strategies for preventing

uma empresa de cibersegurança.

Diferentes e nem sempre iguais

As estratégias e as tecnologias para proteger uma cadeia de fornecimento são, de alguma forma, semelhantes ao que cada organização deve definir para si própria. As estratégias de prevenção e mitigação dos ataques aos fornecedores, parceiros e clientes na cadeia passam pela implementação de políticas internas de cibersegurança (formação e colaboração entre os envolvidos, soluções de monitorização de intrusões, uso da criptografia na proteção dos dados, gestão segura de identidades, entre outras) e com a avaliação de riscos e auditorias regulares aos elementos da cadeia externa de fornecimento.

A adoção de medidas para a antecipação de problemas será uma questão de negócio. "Até 2025, 60% das organizações da cadeia de abastecimento utilizarão o risco da cibersegurança como um fator determinante na realização de transações e de compromissos comerciais com terceiros", antecipa um inquérito da Gartner. Há uma "postura agressiva" dos responsáveis das cadeias de fornecimento, **refere** o analista Brian Schultz. "No entanto, cada nova tecnologia introduz novos parceiros, fornecedores e prestadores de serviços na cadeia de fornecimento digital. A implicação para o risco de cibersegurança é um número cada vez maior de novos caminhos para possíveis ataques de atores maliciosos".

and mitigating attacks on suppliers, partners and customers in the chain involve implementing internal cybersecurity policies (training and collaboration between those involved, intrusion monitoring solutions, the use of cryptography to protect data, and secure identity management, among others) and carrying out regular risk assessments and audits to the elements of the external supply chain.

Adopting measures to anticipate problems will be a business decision. 'By 2025, 60 % of supply chain organisations will use cybersecurity risk as a significant determinant in conducting third-party transactions and business engagements,' a Gartner survey predicts. There is an 'aggressive stance' from supply chain managers, **says** analyst Brian Schultz. 'However, each new technology introduces new partners, vendors and service providers into the digital supply chain. The implication for cybersecurity risk is an ever-growing number of new pathways to potential attacks from malicious parties.'

As recent cases about the difficulty of controlling all elements of the supply chain show, this may be the main weakness in cybersecurity. But the realisation of this danger is not new.

A decade ago, 'about 80 percent of data breaches originate in the supply chain,' **told**

Como demonstram os recentes casos sobre a dificuldade em controlar todos os elementos da cadeia de abastecimento, esta pode ser o principal ponto fraco na cibersegurança. Mas a perceção desse perigo não é recente.

Há uma década, "cerca de 80% das violações de dados têm origem na cadeia de fornecimento", afirmava Torsten George, da empresa de software Agiliance. "Os piratas informáticos começaram a procurar o ponto mais fraco da cadeia, que é o fornecedor".

Em 2019, essa percentagem diminuiu para 50% de ataques que "não procuram apenas uma rede alvo, mas também as que estão ligadas através de uma cadeia de fornecimento". Entre esse ano e 2023, a Sonatype registou 245 mil ciberincidentes.

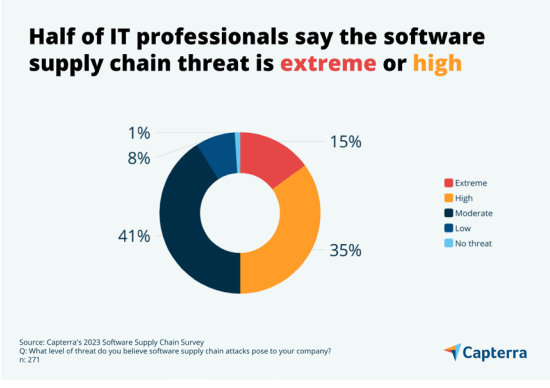
O ataque a 18 mil clientes do fornecedor de gestão de redes SolarWinds marcou o ano 2020, com cerca de 250 organizações afetadas após os atacantes acederem a diferentes níveis da sua cadeia de abastecimento. O ataque foi considerado "uma cibercatástrofe do ponto de vista da segurança nacional" dos EUA, com uma estimativa de perdas seguradas de 90 milhões de dólares.

Um inquérito da Capterra a mais de 220 organizações revelou que 61% foram "afetadas por uma ameaça à cadeia de abastecimento [em 2022], validando as preocupações crescentes e justificando uma resposta forte tanto das empresas como do governo". Quanto

Torsten George of the software company Agiliance. 'Hackers began looking for the weakest point in the chain, and that's the supplier.'

In 2019, that percentage dropped to 50 per cent of attacks that 'are after not only one target network but also those that are connected via a supply chain.' Between that year and 2023, Sonatype recorded 245 000 cyber incidents.

The attack on 18 000 customers of network management provider SolarWinds marked 2020, with around 250 organisations affected after the attackers accessed different levels of their supply chain. In the USA, the attack was considered 'a cyber catastrophe from a national security perspective', with an estimated insured loss of $90 million.



A Capterra survey to more than 220 organisations showed that 61 % have been 'affected by a supply chain threat in 2022, validating growing concerns and justifying a

às "39% sortudas" que passaram incólumes a ataques, "é provável que tenha sido mais sorte do que qualquer outra coisa".

Por fim, a consultora Juniper Research **calculou** que o custo global dos ciberataques às cadeias de fornecimento em 2023 atingiu os 45,8 mil milhões de dólares, devendo aumentar para os 80,6 mil milhões em 2026, devido aos "riscos crescentes decorrentes da ausência de processos de segurança da cadeia

strong response from both businesses and the government.' As for the 'lucky 39 %' who made it through the attacks unscathed, 'it's likely luck more than anything.'

Finally, consultancy Juniper Research **calculated** that the total cost of cyberattacks on supply chains in 2023 reached $45.8 billion dollars, and is expected to rise to $80.6 billion in 2026, due to the 'increasing risks from absent software supply chain security

A importância de uma IoT segura na "supply chain"

Os dispositivos da Internet of Things (IoT) generalizaram-se e, apesar da tentativa de imposição de regras restritas nas organizações, são usados sem grandes preocupações de segurança. Para garantir uma maior proteção a estes dispositivos, pode adotar algumas medidas:

- Instalar software de segurança nos dispositivos e nos sistemas em rede aque estão ligados, para proteger contra malware, vírus e quaisquer tentativas de ataques maliciosos.
- Atualizar regularmente o software e o firmware dos dispositivos.
- Encriptar os dados armazenados nos dispositivos IoT.
- Implementar medidas de segurança, como firewalls.
- Utilizar ferramentas de gestão de dispositivos para os monitorizar.
- Definir políticas e procedimentos de segurança para limitar o acesso a dispositivos e a dados.

Fonte: IT Supply Chain

The importance of a secure IoT in the supply chain

Internet of Things (IoT) devices have become widespread and, despite attempts to impose strict rules on organisations, are used without major security concerns. To ensure greater protection for these devices, you can adopt a few measures:

- Install a security software on the devices and the networked systems they are connected to, to protect against malware, viruses and any attempted malicious attacks.
- Regularly update the software and firmware on the devices.
- Encrypt data stored on IoT devices.
- Implement security measures, such as firewalls.
- Use device management tools to monitor devices.
- Define security policies and procedures to limit access to devices and data.

de fornecimento de software e à complexidade crescente [dessas] cadeias em geral".

No mais recente "Data Breach Investigations Report", a Verizon define o conceito como uma "violação envolvendo terceiros, que inclui infraestruturas de parceiros afetadas e problemas diretos ou indiretos na cadeia de fornecimento de software - incluindo quando uma organização é afetada por vulnerabilidades em software de terceiros".

A operadora norte-americana antecipa que estas falhas de segurança cheguem aos 15% do total, um crescimento de 68% relativamente ao ano anterior, "impulsionado sobretudo pela utilização de 'exploits' de dia-zero para ataques de ransomware e de extorsão".

Este cenário representa "uma falha na resiliência da comunidade e no reconhecimento de como as organizações dependem umas das outras" e não devem premiar os elos mais fracos da cadeia.

Pelas complexas interdependências estabelecidas com os alvos, os seus fornecedores e os clientes, a cadeia de abastecimento é um alvo interessante para ser explorada para ciberataques. As organizações devem, por isso, atentarem nas políticas de segurança internas e com o exterior. Como refere o documento da Verizon, estes ataques são também "violações que uma organização poderia potencialmente atenuar ou evitar se tentasse selecionar fornecedores com melhores registos de segurança".

processes, and the rising complexity of software supply chains overall.'

In the latest 'Data Breach Investigations Report', Verizon defines the concept as a 'breach involving a third party that includes partner infrastructure being affected and direct or indirect software supply chain issues - including when an organization is affected by vulnerabilities in third party software.'

The US operator expects these security breaches to reach 15 % of the total, a increase of 68 % on the previous year, 'driven above all by the use of zero-day exploits for ransomware and extortion attacks.'

This scenario represents 'a failure of community resilience and recognition of how organisations depend on each other', so they must not reward the weakest links in the chain.

Due to the complex interdependencies established with the targets, their suppliers and customers, the supply chain is an interesting target to exploit for cyberattacks. Organisations must therefore pay attention to their internal and external security policies. As the Verizon document points out, these attacks are also 'breaches an organization could potentially mitigate or prevent by trying to select vendors with better security track records'.

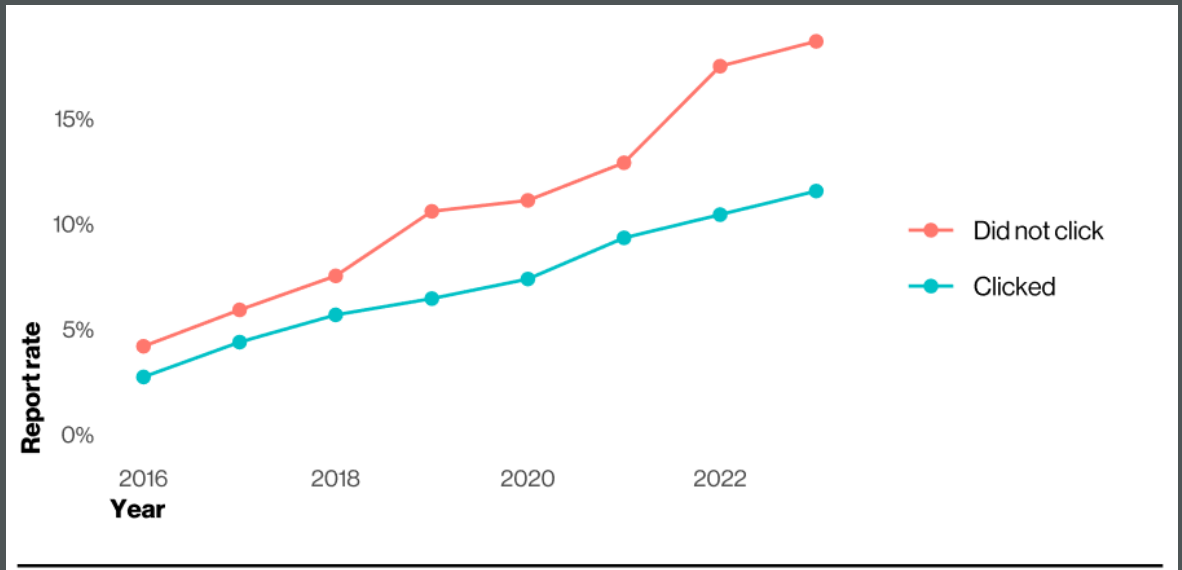


Figure 40. Phishing email report rate by click status

Um minuto para o phishing ter sucesso

Os ataques de phishing acontecem rapidamente: o tempo médio para os utilizadores abrirem emails de phishing é de menos de um minuto. 20% sabe identificar a existência de phishing, mas 11% dos utilizadores clica nesse tipo de email, revela o 2024 Data Breach Investigations Report.

Os maiores pedidos de ransomware

63% dos pedidos de ciber-resgate a 1.701 organizações que tiveram os seus dados cifrados ultrapassaram os mil milhões de dólares (o valor médio total foi de 4.321 milhões. 34% das organizações afetadas demorou mais de um mês a recuperar, perante os 24% do ano anterior, de acordo com o The State of Ransomware 2024 da Sophos.

One minute for phishing to succeed

Phishing attacks happen quickly: the average time for users to open phishing emails is less than one minute. 20 % know how to identify the existence of phishing, but 11 % of users click on this type of email, reveals the 2024 Data Breach Investigations Report.

The largest ransomware requests

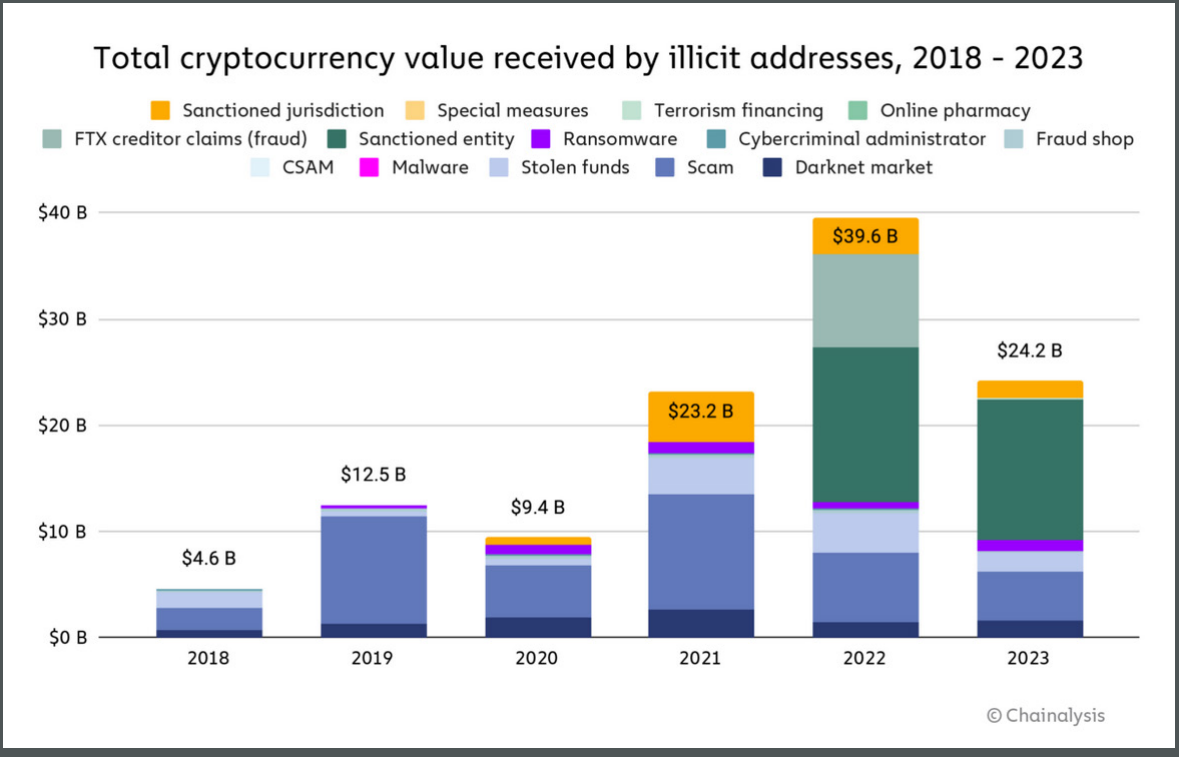
63 % of ransom demands from 1 701 organisations that had their data encrypted exceeded $1 billion (the total average value was $4.321 million). 34 % of the organisations affected took more than a month to recover, compared to 24 % the previous year, according to Sophos' The State of Ransomware 2024.

Criptomoeda ilícita deverá aumentar

O valor global das criptomoedas provenientes de fontes ilegais caiu para os 24,2 mil milhões de dólares em 2023 (o valor reflete as perdas de 8,7 mil milhões relativos à FTX) mas antecipa-se que o "cripto Inverno" está a acabar e se vai assistir a um crescimento, refere o 2024 Crypto Crime Trends da Chainalysis.

Illicit cryptocurrency expected to grow

The global value of illicit cryptocurrency fell to $24.2 billion in 2023 (the figure reflects losses of 8.7 billion against FTX) but the 'crypto winter' is expected to end soon and a new growth may soon be upon us, says Chainalysis' 2024 Crypto Crime Trends.



3

Luisa Ribeiro Lopes

Presidente do Conselho Diretivo Executivo do .PT
Chairman of the .PT Executive Board

1. Como surgiu a iniciativa de estabelecer a cooperação entre o .PT e a Polícia de Segurança Pública (PSP) e estão previstos novos protocolos com outras entidades?

O aumento atual do cibercrime está a impactar o mundo inteiro, e Portugal não é exceção. Em 2022, o país registou mais de 3.500 incidentes de cibersegurança, refletindo uma tendência de grande crescimento. Esse incremento está diretamente ligado aos avanços tecnológicos, que, embora tragam inúmeras facilidades e inovações, também abrem portas para novas formas de ameaças digitais.

O protocolo de cooperação entre o .PT e a PSP surgiu como resposta a estes problemas, uma vez que combater estas ameaças exige um trabalho conjunto, uma expertise partilhada e uma visão estratégica comum, visando a promoção de um ciberespaço mais seguro tanto para os cidadãos como para as empresas portuguesas.

1. How did the initiative to start a co-operation between .PT and the Portuguese Public Security Police (PSP) come about and are there new protocols with other entities planned?

The current increase in cybercrime is impacting the entire world, and Portugal is no exception. In 2022, Portugal recorded more than 3 500 cybersecurity incidents, reflecting an upward trend. This increase is directly linked to technological advances which, while bringing countless facilities and innovations, also open doors to new forms of digital threats.

The co-operation protocol between .PT and the PSP came about as a response to these problems. Fighting these threats requires joint work, shared expertise and a common strategic vision, aimed at promoting a safer cyberspace for both Portuguese citizens and companies.

The .PT statutes provide for partnerships to be developed with renowned Portuguese organisations, such as this protocol established with the PSP. We are working to establish new protocols with other organisations in order to keep cyberspace safe. This effort also involves training citizens and companies, since the better we understand cybersecurity threats, the better we understand how to protect ourselves.

Os estatutos do .PT preveem que sejam desenvolvidas parcerias com entidades de renome a nível nacional, como o protocolo estabelecido com a PSP. Desta forma estamos a trabalhar para desenvolver novos protocolos com outras entidades por forma a manter o ciberespaço seguro, o que também passa pela capacitação dos cidadãos e das empresas, visto que quanto melhor compreendermos as ameaças de cibersegurança, melhor percebemos o que temos de fazer para nos protegermos.

2. Quais são as áreas de cooperação identificadas no protocolo que podem contribuir para o combate à cibercriminalidade e reforço da cibersegurança em Portugal?

Enquanto entidade gestora do domínio de topo de Portugal, o .PT monitoriza as tendências, identifica vulnerabilidades e trabalha diariamente de forma a garantir a segurança e a resiliência da infraestrutura digital do país. A PSP é uma entidade com mais de 150 anos de experiência no combate ao crime em várias vertentes, incluindo atualmente o cibercrime.

Desta forma, acreditamos que uma colaboração entre o conhecimento técnico do .PT e a experiência operacional da PSP permitirá fortalecer as defesas digitais do nosso país, proteger os cidadãos e as empresas, garantindo que a transição digital seja cada vez mais segura e de confiança.

2. Which areas of cooperation identified in the protocol can contribute to fighting cybercrime and strengthening cybersecurity in Portugal?

As the managing body of Portugal's top-level domain, .PT monitors trends, identifies vulnerabilities and works daily to ensure the security and resilience of the country's digital infrastructure. The PSP is an organisation with more than 150 years' experience in fighting crime on various fronts, including cybercrime.

Therefore, we believe that a collaboration between .PT's technical knowledge and the PSP's operational experience will strengthen our country's digital defences, protect citizens and businesses, and ensure that the digital transition is increasingly secure and reliable.

This collaboration protocol aims to implement an effective strategic development in the fight against cybercrime, design combat operations, train and qualify people, develop specific tools to support investigations, and other areas of the fight against cybercrime that may be agreed between both organisations. These areas of co-operation aim to increase prevention and the ability to fight cybercrime by exchanging knowledge and training people.

Este protocolo de colaboração pretende implementar um efetivo desenvolvimento estratégico no combate ao cibercrime, conceber operações de combate, formar e qualificar pessoas, desenvolver ferramentas específicas de apoio à investigação, e outras áreas de combate ao cibercrime que venham a ser acordadas entre ambas as entidades. Estas áreas de cooperação têm como objetivo aumentar a prevenção e a capacidade de combater a cibercriminalidade, através da troca de conhecimentos e da capacitação das pessoas.

3. Uma das áreas de cooperação do protocolo passa pela "formação e qualificação de recursos humanos". Esta vertente de capacitação será transferida para a sociedade civil?

Estamos cada vez mais confrontados com a necessidade de responder a um conjunto de novos desafios e tendências de transformação digital da economia e sociedade. O papel do Estado continua a ser de extrema importância nesta transição digital, mas cabe também à sociedade civil contribuir para a Estratégia da União Europeia para a Cibersegurança na Década Digital, uma vez que é um pilar fundamental no desenvolvimento do futuro digital da Europa, mas também para colocar Portugal acima da média dos países europeus, garantindo que os cidadãos e empresas portuguesas estejam mais protegidos nesta transformação digital.

3. One of the areas of co-operation in the protocol is 'training and qualification of human resources'. Will this training also reach civil society?

We are increasingly faced with the need to respond to a series of new challenges and trends in the digital transformation of the economy and society. The role of the Portuguese Government remains extremely important in this digital transition, but it is also up to civil society to contribute to the European Union's Cybersecurity Strategy for the Digital Decade; it is a key pillar to develop Europe's digital future and to place Portugal above the European countries' average, ensuring that Portuguese citizens and companies are better protected during this digital transformation.

This goal can only be achieved by training and qualifying people, not forgetting the importance of strengthening the gender

Este desígnio só é possível através da capacitação e qualificação das pessoas, não esquecendo a importância de reforçar o equilíbrio de género em áreas masculinizadas. O protocolo entre o .PT e a PSP tem como propósito reforçar a capacitação e qualificação dos seus recursos humanos, criando profissionais preparados para lidar com incidentes de acordo com as regulamentações e diretrizes, mas também disseminar conhecimento e as melhores práticas para combater o cibercrime na sociedade.

Torna-se imperativo desenvolver parcerias e programas que, para além de combaterem o cibercrime, implementem boas práticas que permitam a prevenção dos mesmos e que capacitem os cidadãos e as empresas para as ameaças e desafios do ciberespaço. Só centrando o espaço digital nas pessoas conseguiremos atingir o propósito desta parceria fundamental na área da cibersegurança.

balance in male-dominated areas. The protocol between .PT and the PSP aims to strengthen the training and qualification of its human resources, creating professionals prepared to deal with incidents in accordance with regulations and guidelines. It also prepares them to disseminate knowledge and best practices to fight cybercrime in society.

It is imperative to develop partnerships and programmes that will, not only fight cybercrime, but also implement good practices to prevent it and empower citizens and companies to deal with the threats and challenges of cyberspace. Only by centring the digital space on people will we be able to achieve the purpose of this fundamental partnership in the area of cybersecurity.

Filipe Frasquilho

Diretor de Serviços de TI da IP Telecom
Director of IT Services at IP Telecom

Os desafios dos Planos de Continuidade de Negócio e das Soluções de Disaster Recovery em particular

No mundo digital atual, a tecnologia é um dos pilares fundamentais para qualquer Plano de Continuidade de Negócio (PCN). As organizações estão cada vez mais digitais e dependem da tecnologia para o seu normal funcionamento ficando, por essa razão, cada vez mais expostas a riscos, como falhas de hardware, software, ataques cibernéticos, entre outros.

Um PCN é uma ferramenta fundamental, que inclui estratégias de continuidade para processos, pessoas e tecnologia. A tecnologia é importante, mas os outros dois pilares são fundamentais para garantir um PCN robusto.

As organizações, de acordo com a sua maturidade, capacidade financeira e Compliance, devem definir as estratégias de continuidade de negócio a implementar e testar. Qualquer estratégia deve incluir, entre outros, os seguintes elementos:

- **Identificação e avaliação dos riscos** que podem afetar o negócio, sejam sistemas e aplicações, pessoas ou processos. Os riscos podem ser internos (ex. falhas de hardware/software) ou externos (ex. desastres naturais ou ataques cibernéticos)

The challenges of Business Continuity Plans and Disaster Recovery Solutions in particular

In today's digital world, technology is one of the key pillars of any Business Continuity Plan (BCP). Organisations are becoming increasingly digital and rely on technology for their day-to-day operation. They are, therefore, increasingly exposed to risks such as hardware and software failures, cyber-attacks, and more.

A BCP is a fundamental tool that includes continuity strategies for processes, people and technology. Technology is important, but the two other pillars are key when it comes to ensuring a robust BCP.

Organisations must define the business continuity strategies to be implemented and tested according to their maturity, financial capacity and compliance. Any strategy must include, among other things, the following elements:

- **identification and assessment of risks** that can affect the business, be they systems and applications, people or processes. Risks can be internal (e.g. hardware/software failures) or external (e.g. natural disasters or cyber-attacks) and

e têm associados a análise de impacto no negócio. Esta análise é fundamental para identificar o que é mais critico e a ordem sequencial da recuperação de modo a ter o menor impacto possível no negócio.

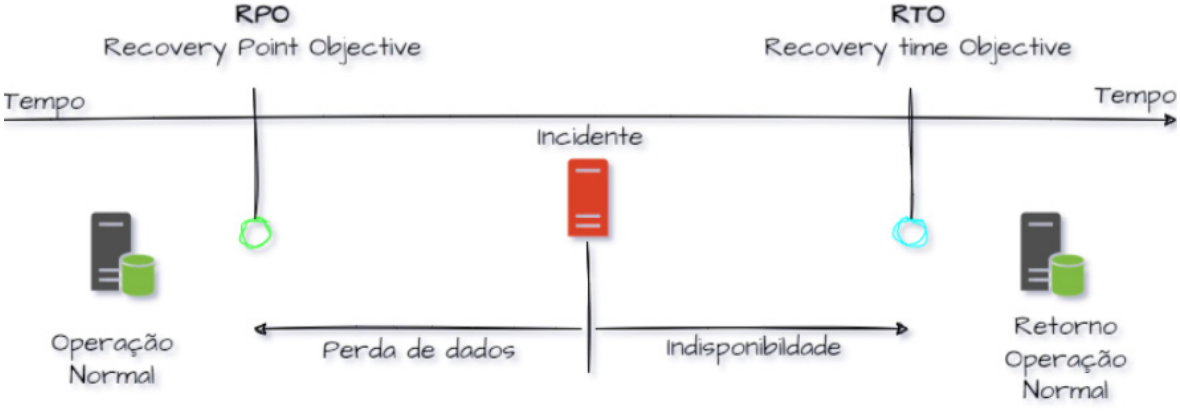
- **Plano de resposta** define as ações que a organização tomará em caso de interrupção, que podem incluir o uso de um sistema de backup, migração para um centro de dados alternativo ou implementação de um plano de contingência.
- **Testes, treino e melhorias:** O plano de resposta deve ser testado e treinado regularmente para garantir que é eficaz, que está atualizado e que responde às necessidades e aos riscos identificados.

A tecnologia é uma peça fundamental para a eficácia do PCN de qualquer organização. O IT Disaster Recovery (DR) é um dos principais instrumentos do PCN, cada vez mais complexo e desafiante, devido à multiplicação de diferentes tecnologias e Cloud Providers que as organizações utilizam. A identificação dos ativos, a sua caraterização e a sua criticidade são fundamentais para a definição dos tempos de recuperação, nomeadamente o Reco-

are associated with analysing the impact on the business. This analysis is essential to identify what is most critical and the sequential order of recovery in order to have the least possible impact on the business.

- **Response plan** to define which actions the organisation will implement in the event of an interruption, which may include using a backup system, migrating to an alternative data centre or implementing a contingency plan.
- **Testing, training and improvements**: The response plan should be tested and trained on a regular basis to ensure that it is effective, that it is up to date and that it responds to the needs and risks identified.

Technology is key when it comes to the effectiveness of any organisation's BCP. IT Disaster Recovery (DR) is one of the BCP's main tools, increasingly complex and challenging due to the multiplication of different technologies and Cloud Providers that organisations use. The identification of assets, their characterisation and criticality are fundamental for defining recovery times,



very Time Objetive (RTO) e o Recovery Point Objective (RPO), dos diferentes sistemas.

O nível mais básico é a recuperação de dados dos sistemas em caso de perda, através de soluções tradicionais de Backup. Pode ser efetuado localmente, noutro local off-site (através de um Cloud Provider) ou em ambos os locais (recomendado). Esta abordagem deve ser testada frequentemente (no mínimo uma vez por mês). De referir que as soluções de Backup servem outros objetivos.

O nível seguinte, mais complexo, é baseado em soluções de DR em modo Stand by que permitem às organizações restaurar os seus sistemas e aplicações noutro local em caso de interrupção e de acordo com os RPO e RTO definidos. Os testes são muito importantes e devem ser efetuados sempre que existam alterações à lista de ativos (ex. a introdução de uma nova aplicação, a sua arquitetura e dependências). As pessoas e os processos são fundamentais e devem fazer parte da amostra de testes.

O cenário ideal será ter um DR Ativo-Ativo, em que não exista a necessidade de efetuar o Rollback aos testes reais realizados.

Apesar do elevado investimento que este cenário normalmente obriga, há enormes vantagens ao nível dos processos e pessoas, pois qualquer teste seria idêntico à realidade, tendo todos os sistemas em funcionamento para todos os utilizadores e sem a necessi-

namely the Recovery Time Objective (RTO) and the Recovery Point Objective (RPO) for the different systems.

The most basic level is the recovery of system data in the event of loss, using traditional backup solutions. This can be done locally, at another off-site location (via a Cloud Provider) or at both locations (recommended). This approach should be tested frequently (at least once a month). It should be noted that backup solutions also serve other purposes.

The next, more complex level is based on standby DR solutions that allow organisations to restore their systems and applications elsewhere in the event of an interruption and in accordance with the defined RPO and RTO. Testing is very important and should be carried out whenever there are changes to the asset list (e.g. introduction of a new application, its architecture and dependencies). People and processes are fundamental and should be part of the test sample.

The ideal scenario is to have an Active-Active DR, where there is no need to roll back the actual tests carried out.

Despite the high investment this scenario normally requires, there are huge advantages in terms of processes and people, as any test would mirror reality, with all systems in operation for all users and without the

dade de efetuar simulações que, na maioria das situações, apenas servem para cumprir com necessidades e obrigações impostas pelo Compliance.

Adicionalmente e com forte crescimento nos últimos anos, as medidas de segurança/cibersegurança são essenciais para proteger os sistemas e aplicações contra ataques cibernéticos. Estas medidas do PCN devem, também, estar previstas em qualquer DR.

As organizações que investem no seu PCN e que efetuem com regularidade os testes estão melhor preparadas para responder a uma disrupção, seja ela por falha, por causas naturais ou por ataque. Um PCN eficaz ajudará a minimizar os impactos financeiros e operacionais de qualquer interrupção.

À medida que a tecnologia continua a evoluir, as organizações devem estar atentas às novas oportunidades para melhorar e tentar simplificar o seu PCN e DR.

need to carry out simulations which, in most situations, only serve to fulfil the needs and obligations imposed by Compliance.

In addition, and with strong growth in recent years, security/cybersecurity measures are essential to protect systems and applications against cyber-attacks. These BCP measures should also be included in any DR carried out.

Organisations that invest in their BCP and regularly test it are better prepared to respond to a disruption, be it due to failure, natural causes or an attack. An effective BCP will help minimise the financial and operational impacts of any disruption.

As technology continues to evolve, organisations should be on the lookout for new opportunities to improve and try to simplify their BCP and DR.

Caracterização do Ecossistema Industrial do Digital em Portugal

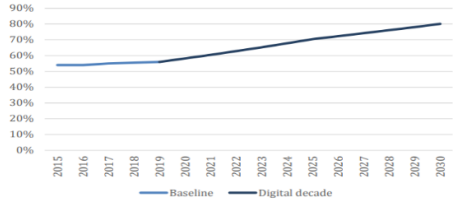
The Digital Industrial Ecosystem in Portugal

***Digital Decade*: População digitalmente qualificada e profissionais digitais altamente qualificados**

Competências digitais básicas

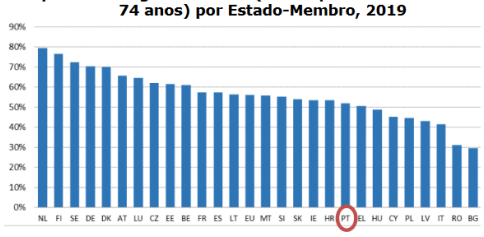
Meta: 80% das pessoas entre os 16 e os 74 anos têm pelo menos competências digitais básicas na UE27
Referência (2019): 53% na UE27

Percentagem de adultos com pelo menos competências digitais básicas (trajetória da UE até 2030)



Fonte: Análise da Comissão Europeia, baseada em Dados do Eurostat

Competências digitais básicas (% das pessoas entre os 16 e os 74 anos) por Estado-Membro, 2019

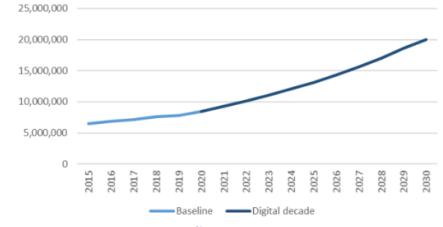


Fonte: Eurostat

Especialistas em TIC

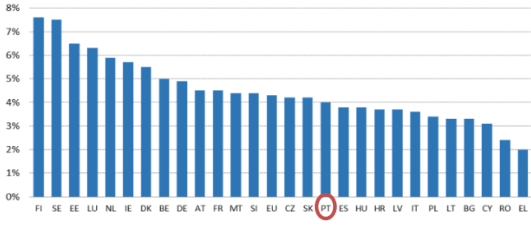
Meta: 20 milhões de especialistas em TIC empregados, com convergência entre mulheres e homens na UE27
Referência (2020): 8,4 milhões de especialistas em TIC empregados, sendo 19% mulheres na UE27

Número de especialistas em TIC empregados (projeção da UE para 2030)



Fonte: Análise da comissão Europeia baseada em Dados do Eurostat

Especialistas em TIC (% de indivíduos empregados entre 15 e 74 anos) por Estado-Membro, 2020



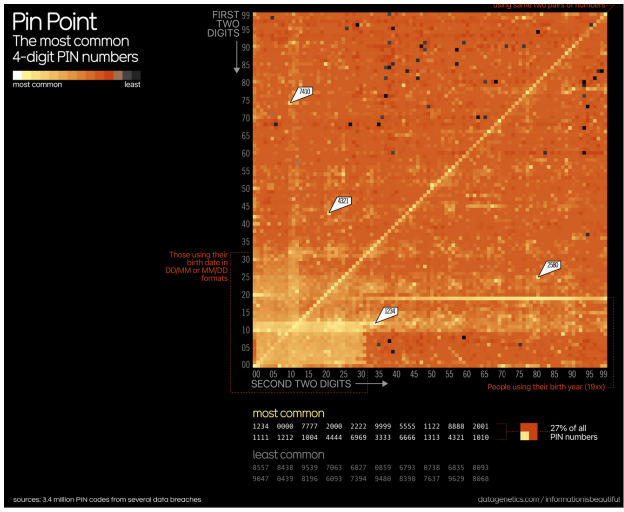
Fonte: Eurostat

Os PINs mais previsíveis

"Existem 10.000 combinações possíveis dos dígitos 0-9 para formar um código PIN de 4 dígitos. Destes dez mil códigos, qual é o menos utilizado", o menos ou o mais previsível?

The most predictable PIN number

"There are 10,000 possible combinations that the digits 0-9 can be arranged to form a 4-digit pin code. Out of these ten thousand codes, which is the least commonly used", the least or the most predictable?



Quantos centros de dados têm as grandes empresas tecnológicas?

"Não existe um padrão único para o tamanho de um centro de dados, pelo que a quantidade não se traduz automaticamente numa maior capacidade".

How many data centres do the big tech companies have?

"There's no one standard of how big a data center needs to be, so quantity doesn't automatically translate into greater capacity".

Diretora | Director
Inês Esteves

Edição | Editor
Pedro Fonseca

Design Gráfico | Graphic Design
Sara Dias
Maria Cristóvão

Tradução | Translation
Sara Pereira

Fotografia | Photography
Capa/Cover: Risto Kokkonen | Unsplash
Índice/Table of contents: Sufyan | Unsplash

Publicação trimestral | Quarterly publication
Julho 2024 | July 2024