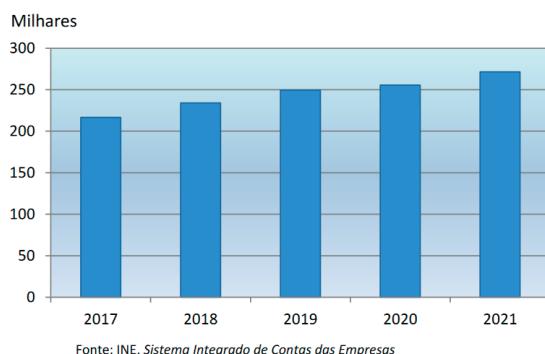


Mais empresas e mais pessoas no setor das TIC em Portugal

Evolução do pessoal ao serviço nas empresas dos setores de alta e média alta tecnologia



O número das empresas tecnológicas em Portugal tem vindo a aumentar e há mais profissionais ao serviço dessas organizações. Dados de 2021 registavam 29,1 mil empresas nos setores de alta e média alta tecnologia, com 271,5 mil trabalhadores – correspondendo a um aumento de mais de 6,7 mil empresas e a mais de 54,8 mil trabalhadores entre 2017 e 2021.

Os dados constam do relatório sobre emprego e formação do Centro de Relações Laborais (CRL), que mostram 144,9 mil pessoas em empresas de tecnologia de informação e comunicação (TIC).

Fonte: [Centro de Relações Laborais](#)

“Discrepâncias” geram ataque à Revolut

O sistema de pagamentos Revolut foi atacado entre o final de 2021 e início de 2022, tendo sido roubado em mais de 20 milhões de dólares. O caso só foi divulgado agora e deveu-se, alegadamente, a “discrepâncias entre os sistemas da Revolut nos EUA e na Europa, fazendo com que fundos fossem erradamente reembolsados utilizando dinheiro [da empresa] quando algumas transações eram recusadas”.

Fonte: [The Hacker News](#)



NATO preocupada com cibersegurança coletiva

A NATO reconheceu na recente reunião de Vilnius estar determinada a empregar todas as suas “capacidades para dissuadir, defender e contrariar todo o espectro de ciberameaças, incluindo através da consideração de respostas coletivas. Um conjunto isolado ou cumulativo de ciberactividades maliciosas poderá atingir o nível de ataque armado e levar o Conselho do Atlântico Norte a invocar, caso a caso, o artigo 5º”. A organização anunciou o lançamento da nova Virtual Cyber Incident Support Capability (VCISC) para apoiar os esforços nacionais em resposta a ciberatividades maliciosas, e a realização da sua primeira Cyber Defence Conference, em novembro próximo.

Fonte: [NATO](#)

MOVEit, um novo tipo de ransomware

O ataque em massa com a ferramenta de transferência de ficheiros MOVEit tem vindo a aumentar o número de vítimas, desde a cadeia de hotéis Radisson à banca, imobiliárias e várias universidades, uma biofarmacêutica ou a empresa de GPS TomTom. O grupo Cl0p, responsável pelos ataques deste novo tipo de ransomware, afirma ter atingido centenas de vítimas. A Emsisoft aponta para 270 organizações e mais de 17 milhões de vítimas individuais.

Fontes: [TechCrunch](#), [Dark Reading](#), [Ars Technica](#)



Foto: [Mohamed Hassan](#), Pixabay

EUA: “roadmap” para a cibersegurança

O Gabinete do Diretor Nacional de Cibersegurança dos EUA revelou o plano de implementação da estratégia nacional de cibersegurança, com prazos para as agências governamentais avançarem com “mudanças destinadas a tornar a regulamentação da cibersegurança mais robusta e simplificada, aumentando simultaneamente a responsabilidade das empresas na proteção das infra-estruturas críticas contra ciberataques”. E já se conhece o orçamento da cibersegurança dos EUA para 2025.

Fontes: [The Record](#), [White House](#), [CyberScoop](#)

BREVES

- A [insegurança](#) dos novos [domínios .zip](#) e outros potenciais [abusos ao Domain Name System](#) (DNS).
- Para desenvolver uma correta [defesa coletiva contra ciberataques a infra-estruturas críticas](#), as agências governamentais devem alinhar-se em [parcerias público-privadas](#), numa abordagem coerente que capacite os proprietários e os operadores dessas infra-estruturas.
- A [inteligência artificial](#) (IA) pode ser [útil aos programadores](#) das [áreas da cibersegurança](#)? É necessário um [tratado de não proliferação dos sistemas de IA](#)?
- Como a IA pode ajudar na [esteganografia](#), a esconder mensagens secretas em imagens, e ser um [risco](#) para as [organizações](#), nomeadamente nos [ataques por email](#).
- Invertendo a [tendência](#) de há alguns anos, os responsáveis pela cibersegurança nas organizações (CISO) tendem agora a reportar aos CIO e muito menos aos CEO. Apenas 5% o faz, quando eram 11% em 2021.
- Uma centena de organizações pediu aos fabricantes uma [melhor segurança para a IoT](#).
- Quando os [carros autónomos são câmaras de videovigilância](#).

- Porque é que há [tantos fornecedores de cibersegurança](#)?

- Um jornalista descobriu uma [campanha de anúncios no Facebook](#) que usava abusivamente do seu nome e rosto para enganar as vítimas. A rede social declarou ter removido o vídeo com o “deepfake”.

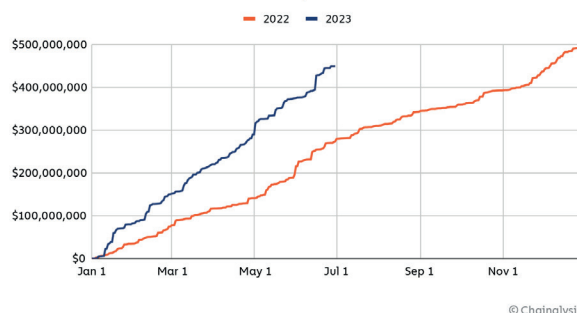
- 449 milhões de dólares foi quanto os grupos de ransomware extorquiram às suas vítimas no primeiro semestre do ano, segundo a monitorização da [Chainalysis](#) a algumas carteiras de criptomoedas. Como se pode [resistir](#)?

- Mais de 300 mil documentos confidenciais de alunos – incluindo relatórios médicos – foram [revelados online](#) após a Minneapolis Public Schools se ter recusado a pagar o resgate de um milhão de dólares requerido por grupos de ransomware.

- No Japão, foi o Porto de Nagoya a sofrer um [ataque de ransomware](#) com impacto nas operações dos terminais de contentores.

- Uma nova vaga de “[pen tests](#)”, conhecidos por Penetration Testing as a Service ([PTaaS](#)), promete reduzir o risco de ciberataques.

Cumulative yearly ransomware revenue, 2022 vs. 2023 (through June)



© Chainalysis

- “Uma [estratégia robusta de backups é uma defesa vital](#) contra os ataques de ransomware” mas as organizações têm de ter em atenção os potenciais ataques a essas cópias de segurança.

- Estão a aumentar os [ciberataques aos smartphones](#), principalmente aos Android.

- Os [hackers também tiram férias](#)...

- Embaixadas e ministérios dos negócios estrangeiros na Europa alvos de [campanha de ciberespionagem](#). E governo inglês foi [atacado pela primeira vez há 20 anos](#)...

- [Nove tipos comuns de malware](#) (e alguns dos piores ataques).

- As [vulnerabilidades mais comuns](#) na cibersegurança e [o que fazer após um ciberincidente](#).

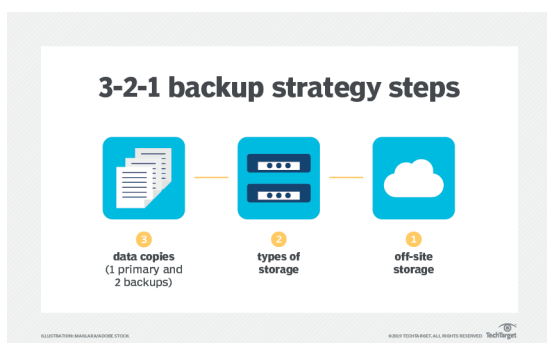
- Compreender os “[frameworks](#)” da cibersegurança (NIST, ISO e outros).

- [Série de vídeos](#) sobre tópicos relacionados com a cibersegurança.

- Como [detetar videocâmaras ocultas](#) nos alojamentos temporários e em hotéis.

- Qual será o impacto de [supertempestades solares](#) que podem causar interrupções na Internet em grande escala, em todo o mundo e durante vários meses?

- O [jogo das passwords](#).



A LER

 [Decreto-Lei n.º 34/2023](#), de 23 de maio, cria a [Cyber Academia and Innovation Hub](#), uma associação de direito privado sem fins lucrativos que, entre outras, terá competências de ligação entre a vertente militar e civil da segurança do ciberespaço.

 Criação do [Centro Europeu de Competências em Cibersegurança](#), previsto no [Regulamento \(UE\) 2021/887](#) do Parlamento Europeu e do Conselho, de 20 de maio de 2021, e que irá gerir projetos com os centros de operações de segurança (SOC) no âmbito da [proposta Cyber Solidarity Act](#).



 [Relatório do Centro Nacional de Cibersegurança](#). O número de incidentes de cibersegurança registados no 1º trimestre do ano recuou 38% face aos valores homólogos registados no mesmo período de 2022. Ainda assim, representa um reforço de 28% quanto comparado com o 4º trimestre.

 [Primeiro relatório da ENISA no setor da saúde](#). A Agência da União Europeia para a Cibersegurança (ENISA) publicou o seu primeiro relatório das ciberameaças no setor da saúde, com o ransomware a representar 54% dessas ameaças.

 [Relatórios da ENISA sobre a inteligência artificial e a cibersegurança](#). A ENISA divulgou quatro relatórios sobre os desafios de maior alcance da IA para a cibersegurança: (1) Multilayer framework for good cybersecurity practices for AI; (2) Cybersecurity and privacy in AI – Forecasting demand on electricity grids; (3) Cybersecurity and privacy in AI – Medical imaging diagnosis; e (4) Artificial Intelligence and Cybersecurity Research.

 [Conclusões do Conselho Europeu sobre a ciberdefesa](#). O Conselho reconhece que as capacidades defensivas da UE são reforçadas pela [Diretiva NIS 2](#) e pela Diretiva sobre a [Resiliência de Entidades Críticas](#) (Diretiva CER), ao mesmo tempo que reitera a sua [Recomendação sobre uma abordagem coordenada da União para reforçar a resiliência das infraestruturas críticas](#).