

Hacking ético sem receios em Portugal

A recente lei que define os objetivos, prioridades e orientações da política criminal para o biénio de 2023-2025 abre a possibilidade de se comunicarem vulnerabilidades à Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), podendo até ser feito de forma anónima.

A lei abrange essa vertente do hacking ético, no âmbito da prevenção da criminalidade, e corresponde ao que desejavam desde 2020 a Associação Portuguesa para a Promoção da Segurança da Informação (AP2SI), o Centro Nacional de Cibersegurança (CNCS), a Comissão Nacional de Proteção de Dados (CNPd) e o Ministério Público (MP).

O “objetivo comum” era “o desenvolvimento de uma Política Nacional de Gestão Coordenada de Vulnerabilidades que incentive investigadores, também conhecidos como hackers éticos, a reportar vulnerabilidades em produtos e serviços sem receio de retaliações”. A nova lei define também que alguns cibercrimes passam a ser de investigação prioritária.

Fontes: [AP2SI](#), [Lei Quadro da Política Criminal para biénio 2023-2025](#)

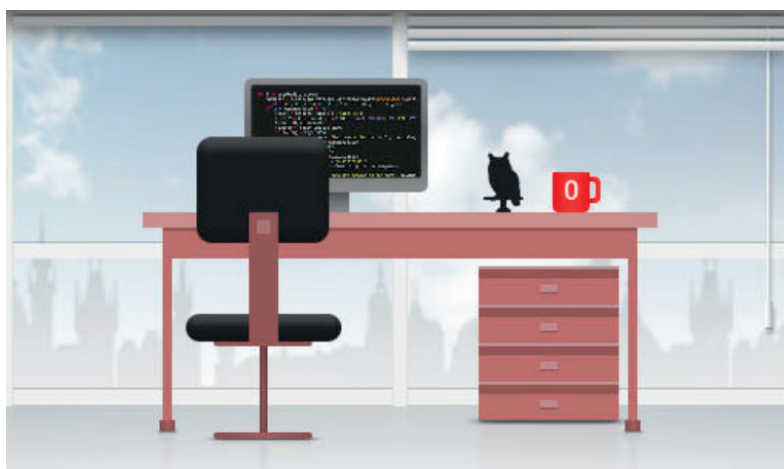
O verão das vulnerabilidades “zero-day”

O número de vulnerabilidades “zero-day” descobertas nos últimos meses levou alguns especialistas a apelidarem-no de “verão quente” das “zero-day”. No entanto, o número das registadas este ano (60) já ultrapassou o total de 52 detetadas em 2022.

São vulnerabilidades que podem ser exploradas para comprometer programas informáticos, obter acesso não autorizado ou para penetrar em redes de comunicações. Uma vulnerabilidade “zero-day” é registada “quando não existe uma solução do fornecedor do software e a vulnerabilidade está a ser ativamente explorada por agentes maliciosos”.

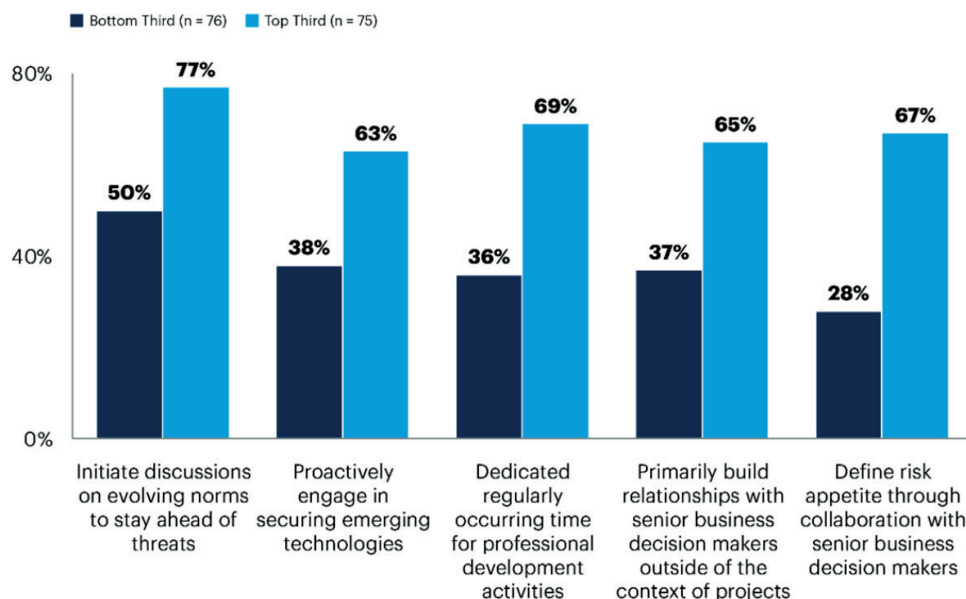
Um especialista em segurança informática considera que “diferente neste verão é que elas são mais impactantes”. Enquanto “nos anos anteriores pode ter havido uma ‘zero-day’ que atingiu uma organização ou uma indústria muito específica, por exemplo”, agora “parece estar muito mais difundido”.

Fontes: [Axios](#), [Zero-day Vulnerability Database](#)



O que faz um CISO ter sucesso?

Effective CISOs' Top Five Game-Changing Behaviors



Source: Gartner (August 2023)

A maioria dos melhores Chief Information Security Officer (CISO) iniciam consistentemente discussões sobre normas em evolução, para anteciparem ameaças, e dedica tempo ao desenvolvimento profissional pessoal, segundo um inquérito a 277 CISOs entre 2020 e 2023. Os mais eficazes também definem os riscos com a contribuição de líderes empresariais seniores, desenvolvem relacionamentos com decisores fora dos projetos e envolvem-se proativamente com tecnologias emergentes.

Fonte: [Gartner](#)

Ciberataques vão ser julgados pelo TPI

O Tribunal Penal Internacional (TPI) vai julgar os crimes da ciberguerra. Os ciberataques da Rússia contra a Ucrânia podem ser dos primeiros casos a ser analisado.

Karim Khan, procurador do TPI, quer investigar cibercrimes que possam violar o Estatuto de Roma, o tratado internacional que define a autoridade do TPI em crimes de guerra, contra a humanidade ou outros.

“A ciberguerra não se desenrola de forma abstrata”, escreveu Khan, e “as tentativas de afetar infra-estruturas críticas, como instalações médicas ou sistemas de controlo para a produção de energia, podem ter consequências imediatas para muitas pessoas, em especial as mais vulneráveis”. O TPI também está atento “à utilização abusiva da Internet para amplificar discursos de ódio e desinformação, que podem facilitar ou levar diretamente à ocorrência de atrocidades”.

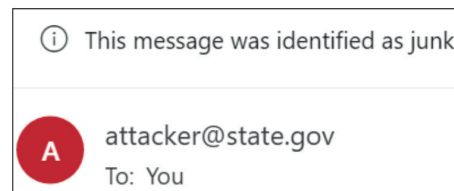
Khan não nomeia países específicos, mas o seu texto surge perante preocupações internacionais com os ciberataques russos à Ucrânia. Em março de 2022, o Centro de Direitos Humanos da Escola de Direito da Universidade da Califórnia em Berkeley enviou um pedido formal ao TPI para os considerar como crimes de guerra.

Fontes: [Ars Technica](#), [Digital Front Lines](#), [NPR](#)

Emails falsos, mas com endereços credíveis

O envio de emails com endereços falsos é mais fácil do que se pensava, devido a falhas no processo que permite o reencaminhamento das mensagens. Segundo uma equipa de investigação da Universidade da Califórnia em San Diego, o problema tem “um amplo impacto” na integridade dos emails enviados de organizações desde o governo dos EUA a empresas de serviços financeiros ou organizações noticiosas.

Através do “forwarding-based spoofing”, os investigadores descobriram poder enviar mensagens como se tivesse origem nessas organizações, contornando as salvaguardas dos fornecedores de email como o Gmail e o Outlook. Nessa situação, “quando os destinatários recebem a mensagem de correio eletrónico falsificada, é mais provável que abram anexos com malware ou que cliquem em ligações que instalam spyware nos computadores”.

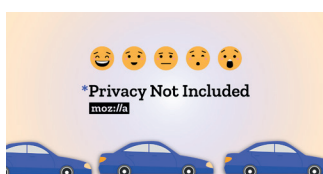
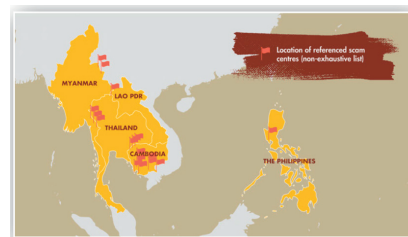


Fonte: [UC San Diego Today](#)

BREVES

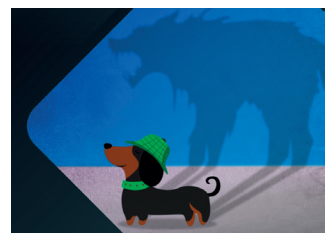
- Portugal ultrapassa a média da UE27 relativamente aos indivíduos com competências acima do nível básico na área da segurança (56% face aos 44% europeus), revela o relatório [“Competências digitais da população e das empresas 2023”](#).
- Só sete seguradoras (de 37 respondentes ao [Questionário Risk Outlook 2.0](#), da ASF) comercializa seguros com cobertura explícita de ciber-riscos. Todas aquelas que o não fazem também não pretendem iniciar qualquer tipo de oferta nesse âmbito.
- O Ransomed usa as leis de proteção de dados como o [RGPD da UE para ameaçar as vítimas](#) com multas se não pagarem um ciber-resgate.
- Os [investigadores da cibersegurança podem ser alvos de atacantes](#) e devem estar atentos às práticas, técnicas e táticas para melhorar a sua própria segurança.
- Quase uma [dezena de empresas de cibersegurança anunciou recentemente despedimentos](#), o que sugere estar a haver uma estabilização na força de trabalho, nomeadamente nas equipas de vendas e de marketing, não afetando diretamente o número de efetivos técnicos. Para estes, o maior problema parece ser o [“burnout”](#).
- [Sem optimismo](#), o [tratado global](#) sobre o [cibercrime](#) pode ser [“desastroso para os direitos humanos”](#).
- Uma análise à evolução do ransomware desde os anos 80 e as [novas ameaças](#), que podem passar pelas criptomoedas e “mecanismos de consenso” utilizados.
- No primeiro semestre do ano, as [organizações de serviços críticos de infraestrutura de TI](#) no Reino Unido reportaram 13 ciberincidentes às autoridades - um aumento significativo em relação às quatro interrupções registadas em 2022 e em 2021.
- Há um [aumento acentuado](#) na distribuição de malware “infostealer”, revela o estudo [“Stealers Are Organization Killers”](#), e os incidentes mais do que duplicaram no primeiro trimestre de 2023 relativamente ao período homólogo do ano passado.

- As [extensões dos browsers](#) espiam mesmo que os seus programadores não o façam.
- A Pandora, uma variante da botnet Mirai, está a ser usada para se infiltrar em [televisores e caixas de TV com Android](#) e servir para ataques distribuídos de negação de serviço (DDoS).
- O atual cenário das ciberameaças no “[2023 H1 Global Threat Analysis Report](#)”.
- A Cimeira da NATO de Vilnius, em julho passado, serviu como fundo para [operações de influência](#) alegadamente russa visando condicionar as conversas online sobre o evento e o país anfitrião, a Lituânia.
- Usando ameaças, tortura e violência sexual, [ganges no Sudeste Asiático forçam](#) milhares de pessoas a participar em burlas internacionais, segundo as [Nações Unidas](#).
- [Cibercriminosos atacaram dois telescópios](#) e forçaram o seu encerramento. Desconhece-se a natureza ou a origem dos ciberataques.
- [Como](#) o FBI [desativou](#) a botnet [Oakbot](#).
- A Microsoft foi [criticada](#) (e [investigada](#)) por práticas de segurança do Azure e outras [ofertas na cloud](#), [acusada](#) de ser “[grosseiramente irresponsável](#)”, estar mergulhada numa “cultura de ofuscação tóxica” e de [não resolver problemas de ransomware](#) ou [no Skype](#). A empresa [divulgou](#) 15 vulnerabilidades em ferramentas usadas para [ataques a sistemas de controlo industrial](#).
- Cibercriminosos estão a [vender endereços de email de membros das autoridades](#) para obter dados pessoais em aplicações de redes sociais.
- [Boas práticas no uso do email](#) para evitar ataques de ransomware às organizações.
- A [cibersegurança necessitará sempre de mais do que soluções técnicas](#).
- As tendências de ciberataques são uma [ameaça sem precedentes às infra-estruturas críticas](#), como a rede elétrica, mas “os serviços públicos enfrentam sérias dificuldades em encontrar e manter os profissionais qualificados necessários para se defenderem”.
- A [cibersegurança, as alterações climáticas e a promoção da sustentabilidade ambiental](#) passam por olhar para a pegada carbónica da segurança da informação, a redução do consumo energético, o aprovisionamento sustentável, a proteção de infraestruturas críticas contra catástrofes climáticas e o apoio a sistemas de energias renováveis.
- Na [segurança das redes 5G](#), “as organizações podem estar à espera de uma rede segura por defeito, mas ainda há muito a fazer”.



- A análise [*Privacy Not Included](#) revela que nenhuma das 25 marcas de automóveis analisadas cumpre as normas mínimas de segurança da Mozilla.
- A evolução para os [serviços móveis e “contactless” na indústria hoteleira](#) torna os seus estabelecimentos mais vulneráveis às ciberameaças, com quase 60 ataques a hotéis este ano. Os cibercriminosos também estão a explorar a [Airbnb para actividades fraudulentas](#).

- As táticas dos burlões nas [fraudes do romance online](#) e como se defender.
- A história do “toolkit” de malware [Decoy Dog](#) revela a eficácia do DNS na deteção e resposta a ameaças.
- [NoName057\(16\)](#), um “lobo solitário” pouco emotivo nos ataques de DDoS.
- [Neo_Net](#), o rei do cibercrime espanhol.
- O [ChatGPT](#) na [investigação](#) forense [digital](#).
- O fim anunciado da “[Infosec Twitter](#)”.
- Está o [hacktivismo a desaparecer](#) ou apenas a diminuir?
- [Boas práticas](#) na [segurança](#) das [APIs](#).
- Cinco histórias positivas de [cibersegurança na região Ásia-Pacífico](#).
- [Shadow IT](#) versus [Shadow AI](#).
- Quais são as [preocupações imediatas dos CISOs](#) com a inteligência artificial e que medidas estão a tomar para as resolver.
- As [motivações para os cibercriminosos](#) inventarem “leaks” de dados podem ajudar os investigadores.



A LER

-  [Lei dos Serviços Digitais entra em vigor no espaço europeu.](#)
-  [A Comissão Europeia avalia ENISA e o quadro de certificação de cibersegurança da UE, conforme exigido no Regulamento Cibersegurança.](#)
-  [Luta contra a cibercriminalidade: quais são as novas leis de cibersegurança da UE?](#)
-  3ª edição do [Inquérito sobre os profissionais de cibersegurança e segurança da informação em Portugal](#) decorre até 23 de setembro.
-  Portugal enviou à CE as suas [Prioridades para o Programa de Trabalhos da CE para 2024](#), onde inclui uma iniciativa para a regulação, conservação, tratamento e acesso a metadados.
-  [Lei relativa à governação dos dados](#): logótipos comuns para identificar facilmente os intermediários de dados de confiança da UE e as organizações de altruísmo para a reutilização de dados.