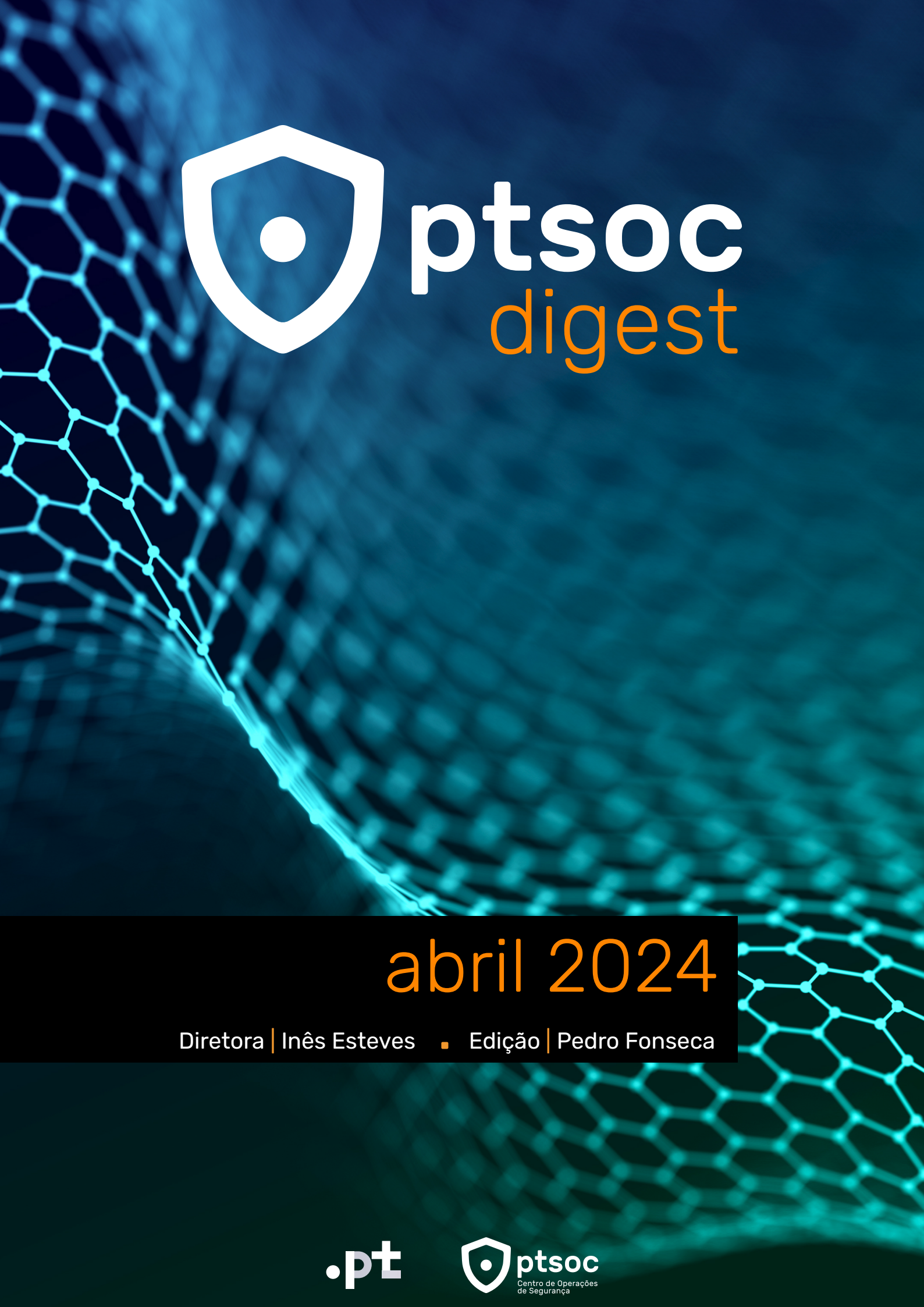


ptsoc digest

abril 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt

ptsoc
Centro de Operações de Segurança

À procura de um espaço digital seguro

O "zero draft" do Global Digital Compact, que teve as contribuições nacionais do .PT e da Anacom no processo de consulta pública, agrega-se em cinco compromissos: superar a exclusão digital e acelerar para os objetivos de desenvolvimento sustentável (ODS); expandir as oportunidades para a inclusão na economia digital; garantir um espaço digital inclusivo, aberto, seguro e protegido; avançar numa governação internacional equitativa dos dados; e governar as tecnologias emergentes, incluindo a inteligência artificial, para a humanidade.

A iniciativa surge quando se analisam os problemas para conseguir uma entidade única responsável pela manutenção e segurança da Internet, como nota a Global Cyber Alliance ou a Common Good Cyber. Entretanto, as negociações para uma nova Convenção do Cibercrime das Nações Unidas terminaram sem consenso e a votação adiada.

Fontes: "Zero draft", Global Digital Compact, Dark Reading, Global Cyber Alliance, Common Good Cyber, Digital Watch

As apostas na cibersegurança do Governo

No âmbito do seu Programa, aprovado em Conselho de Ministros e discutido no Parlamento, o Governo pretende consensualizar a revisão da Estratégia Nacional de Segurança no Ciberespaço, "adotar adequadamente" a NIS2; dotar o Centro Nacional de Cibersegurança de recursos adequados e reforçar a cooperação do CNCS com o SIS.

Propõe-se ainda "combater o cibercrime e as ameaças híbridas, como a desinformação, a propaganda e a interferência eleitoral", nomeadamente pela "utilização ilegítima de plataformas digitais".

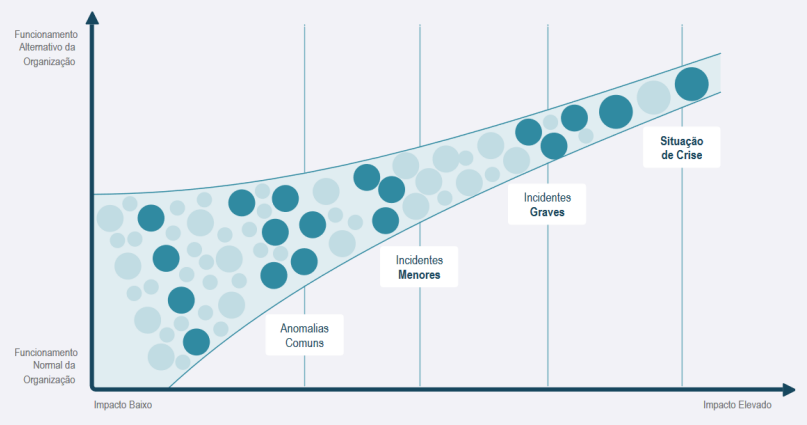
Hartono, Unsplash

Na Administração Pública (AP), quer "progredir" na digitalização, desmaterialização de processos, desenvolvimento tecnológico, reforço da cibersegurança, e integração de ferramentas" de inteligência artificial (IA).

O Executivo quer ainda "maximizar a resiliência cibernética da AP e local", com sistemas de gestão de segurança da informação; garantir a proteção dos dados pessoais e privacidade dos utilizadores online, reforçando os mecanismos de fiscalização, denúncia e sanção, e promover a adoção da encriptação.

Fonte: Programa do XXIV Governo Constitucional

CNCS publica Referencial para comunicação em crises de cibersegurança



O Centro Nacional de Cibersegurança disponibilizou um Referencial de Comunicação de Risco e Crise em Cibersegurança para ajudar as organizações nacionais a comunicarem mais eficazmente em situações de risco e de crises de cibersegurança.

O documento procura agilizar a comunicação com autoridades, clientes, fornecedores, colaboradores internos e media, entre outros, por forma a "responder aos incidentes de forma adequada" e a gerir a reputação da organização, com a disponibilização de "templates" e passos a seguir para "promover o contínuo aperfeiçoamento dos planos de comunicação".

O Referencial divide-se nas três fases de preparar a comunicação, responder à crise e pontos a melhorar e pode ter uma particular relevância para as entidades com menos competências internas na área de comunicação em cibersegurança.

Fonte: CNCS

Os novos problemas que esperam os poucos CISO

Após o BYOD, a nova vaga do BYOAI sem autorização das chefias vai aumentar o potencial para ciberataques por IA? O problema ocorre quando apenas 5% de 4.000 empresas a nível global assume ter responsáveis de cibersegurança nos seus quadros, e o trabalho dos CISO estar mais dificultado, nomeadamente no quadro regulatório.

Este setor continua a ser um "clube de rapazes". Em Espanha, a engenharia informática é a que tem menos matriculadas (14%). O desinteresse tem paralelo nos rendimentos: apesar das disparidades estarem a diminuir (sobretudo ao nível intermédio), as mulheres ainda ganham menos do que os homens e dificilmente acedem a cargos como Theresa Payton, primeira CIO da Casa Branca.

Além da escassez de quadros, e apesar de ser uma grande preocupação, falta às PMEs uma cultura de cibersegurança. No geral, no Reino Unido, a resposta das empresas aos ciberataques é "surpreendente", apesar dos acionistas gostarem do investimento em segurança. As frágeis PMEs confrontam-se ainda com o roubo de identidades por cibercriminosos a usar a (preocupante) IA. Como afirma um responsável do setor, "agora quase todos conseguem fazer os ciberataques mais sofisticados que existem".

Fontes: BYOD, Axios, Diligent Institute, CSO (1, 2, 3, 4, 5), Dark Reading (1, 2, 3), Cybersecurity Dive (1, 2), CyberScoop, Nuevas Realidades, Security Intelligence, Hacker News, Forbes, Eco, The Register, US Chamber

BREVES

• O setor das TI em Portugal tem "uma procura sólida por talentos especializados, o que se reflete em salários competitivos para atrair e manter os melhores profissionais", nota a Adecco no Guia Salarial das Tecnologias de Informação para 2024.

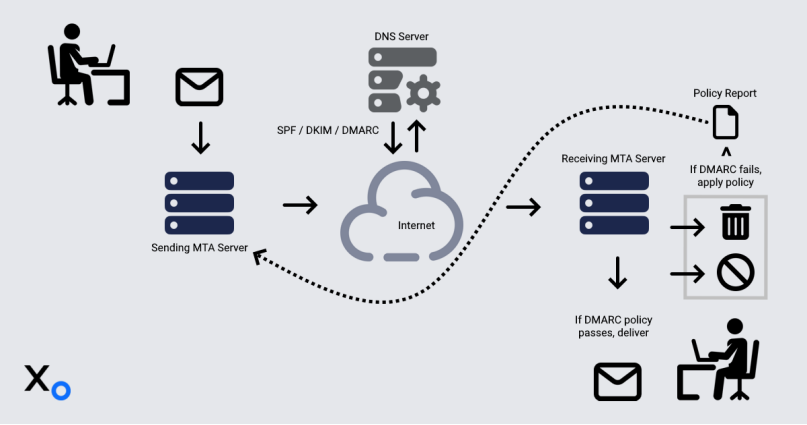
• O SIRESP terá novo presidente, deve evoluir da tecnologia TETRA para LTE/5G e uma fusão entre redes de emergência civil e militar.

• Se o cibercrime fosse um país, seria a terceira maior economia do mundo.

• Google combate o roubo de “cookies” com estratégia das Device Bound Session Credentials (DBSC) e procura ter email mais seguro.

• Reforçar a ciber-resiliência através da colaboração entre entidades públicas e privadas, indivíduos e organizações.

• Parlamento Europeu aprovou normas de ciber-resiliência para proteger produtos digitais de ciberameaças, enquanto a CSA lança um conjunto de normas para a IoT.



• Tendências para os ataques à cibersegurança em 2024.

• Economia do espaço valia 630 mil milhões de dólares em 2023 mas sistemas não são considerados como infraestruturas críticas nos EUA, à semelhança da Europa. Entretanto, já foi lançado um curso de cibersegurança para o espaço.

• O European Union Cybersecurity Certification Scheme for Cloud Services (EUCS) visto pela indústria de serviços e acusado pela falta de referências à soberania dos fornecedores de cloud.

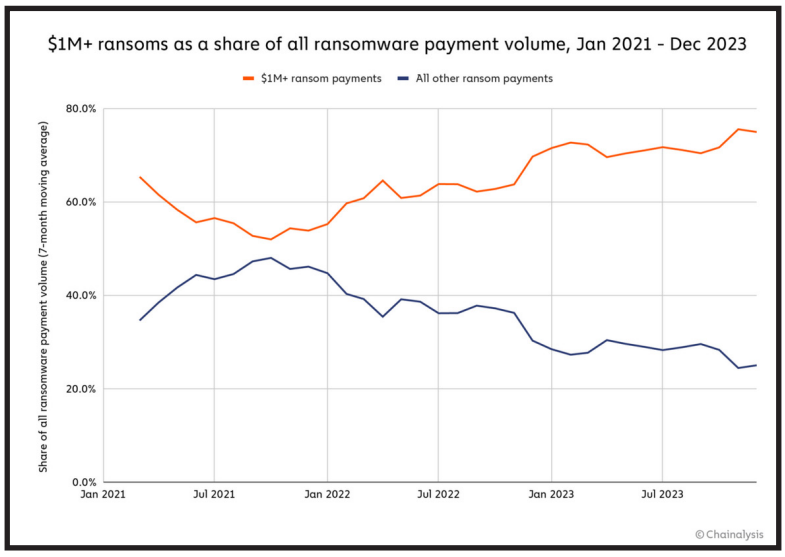
• Calendário e funcionamento da perigosa vulnerabilidade (CVE-2024-3094), descoberta pelo “curioso” Andres Freund no programa em “open source” ZX Utils. A análise de Bruce Schneier.

• UNAPIMON, o malware que se esconde dos programas antivírus.

• Autoridades alertam Microsoft para as falhas de segurança na cloud.

• Apple avisou utilizadores em 92 (ou 150) países para ataques de spyware.

• Cibervigilante ataca Internet da Coreia do Norte e apresenta estratégia à defesa dos EUA, enquanto líder do grupo LockBit revela como as autoridades agiram contra o grupo.



• Ilha de Palau sofre ataque de ransomware reclamado por dois grupos, mas sem forma de pagar resgate a qualquer um.

• Razões para o potencial decréscimo dos ataques de ransomware em 2024, quando o pior pode estar para vir.

• Cibercriminosos distribuem malware em páginas do Facebook disfarçando-se de marcas de software de IA.

• Os “jailbreaks” do ChatGPT estão a ser distribuídos por cibercriminosos em fóruns de atividades maliciosas.

• Os ataques de “phishing” disfarçados de fiáveis sociedades de advogados atacam com malware em diferentes línguas. E sites de obituários estão a ser usados para distribuir malware.

• No primeiro trimestre do ano, a Internet foi interrompida intencionalmente 22 vezes.

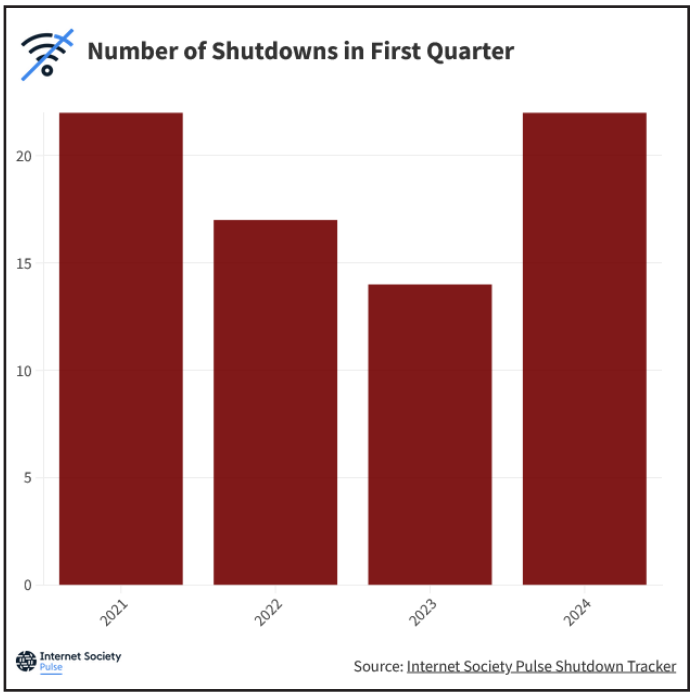
• Em 2023, o Cyber Command dos EUA enviou 22 missões da Cyber National Mission Force para 17 países, tendo partilhado quase uma centena de novos programas de malware com a comunidade de cibersegurança.

• Tabela de preços da Crowdfense para combater vulnerabilidades "zero-day".

• O Open Worldwide Application Security Project (OWASP) alertou os seus "chapters" para um acesso ilegal aos seus dados.

• Ucrânia é palco da primeira "guerra de hackers".

• Como o Mundial de Futebol do Qatar em 2022 podia ter sido "hackado".



LER

Responding to a cyber incident – a guide for CEOs

Foresight Cybersecurity Threats for 2030

Retaliating against cyber-attacks: a decision-taking framework for policy-makers and enforcers of international and cybersecurity law

6G Security White Paper

Review of the Summer 2023 Microsoft Exchange Online Intrusion

Understanding and Responding to Distributed Denial-Of-Service Attacks

Parlamento Europeu adotou o Regulamento da Inteligência Artificial

AI-enabled Crime (vídeo)

Diretora | Inês Esteves

Edição | Pedro Fonseca

Abril 2024