ptsoc digest

março 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt

ptsoc
Centro de Operações de Segurança

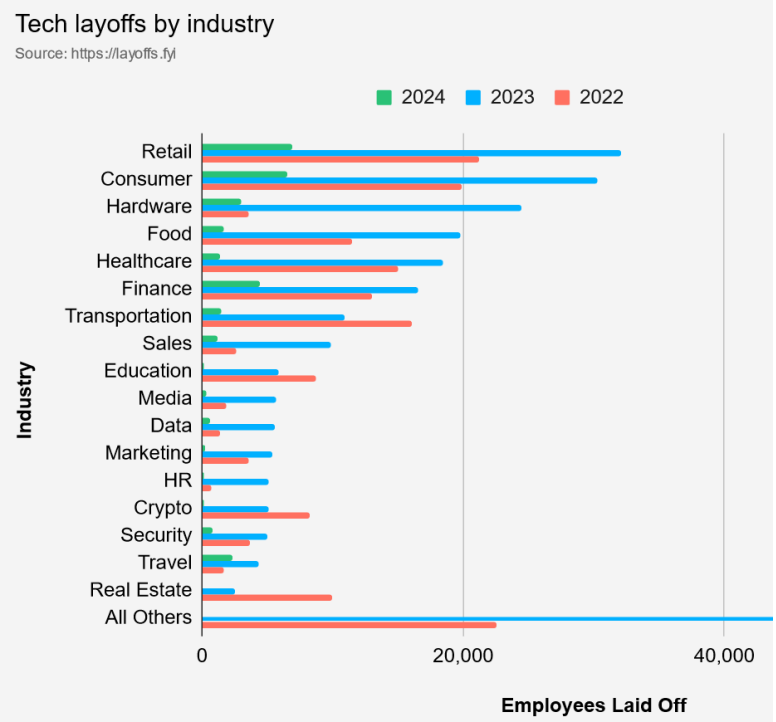
A cibersegurança em Portugal

Decisores de 184 organizações nacionais reconhecem a importância da cibersegurança nas atividades e proteção da sua organização. 45% dos inquiridos para um estudo da Microsoft em Portugal antecipa um investimento futuro em cibersegurança, com 84% a colocar o principal foco no reforço da consciencialização e formação dos colaboradores. Segue-se a avaliação regular dos riscos (69%) e auditorias de segurança ou monitorização de ameaças em tempo real, ambas com 66%.

No passado, metade das organizações investiu mais em cibersegurança, nomeadamente antivírus e malware (81%), medidas de autenticação fortes para acesso a sistemas críticos (71%) e "firewalls" (61%). As entidades expostas a ciberincidentes afirmaram não terem tido perdas financeiras (68%) ou perda de dados (62%), quase a mesma percentagem que considera a comunicação às autoridades como um procedimento normal.

Fonte: Estado da Cibersegurança em Portugal

Desafios para as novas e inúmeras competências dos CISO



Desde o início do ano, foram despedidas mais de 50 mil pessoas em duas centenas de empresas tecnológicas, algo semelhante ao "crash" das .com em 2001, levando muitos profissionais a aceitarem cortes salariais - isto se encontrarem um novo emprego.

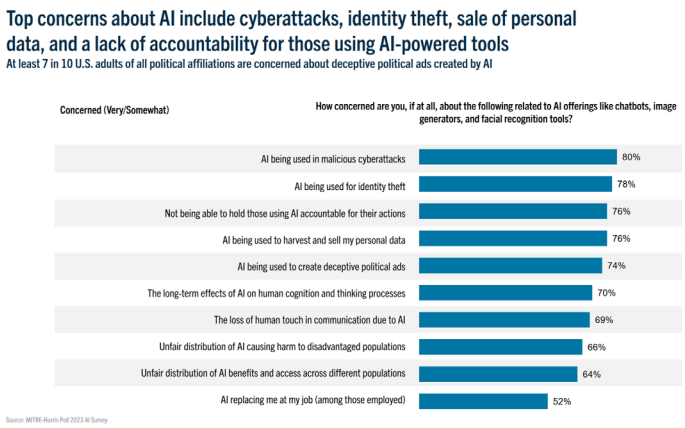
No entanto, alguns empregos de topo na cibersegurança ainda são bem remunerados, a acompanhar as novas exigências requeridas aos CISO. Estes estão agora sempre em evolução, a gerir potenciais ameaças legais, a lidar com uma gestão de competências cada vez mais exigente e diversificada, confrontando-se com ex-profissionais que aderiram ao cibercrime num turbulento ambiente de consolidação onde também imperam os despedimentos.

Mesmo em Portugal, onde os cursos estão a aumentar, continuam a faltar especialistas em cibersegurança. Noutros países, já se questiona uma reciclagem formativa e a contratação de hackers e cibercriminosos como uma potencial solução para a referida escassez de talentos.

Fontes: Laid-off techies face 'sense of impending doom' with job cuts at highest since dot-com crash; 5 of the highest-paying cybersecurity jobs right now; The CISO Role Is Changing. Can CISOs Themselves Keep Up? What Is A Chief Information Security Officer? Beyond the table stakes: CISO Ian Schneller on cybersecurity's evolving role; What Companies & CISOs Should Know About Rising Legal Threats; How cybersecurity roles are changing and what to look for when hiring; Building a robust cyber security workforce; The essential requirements for landing a career in cybersecurity; How gen AI helps entry-level SOC analysts improve their skills; Broke Cyber Pros Flock to Cybercrime Side Hustles; Tips on Managing Diverse Security Teams; Relatório Cibersegurança em Portugal – Sociedade; Help Wanted From Convicted Cybercriminals; Cybersecurity skills gap: Why it exists and how to address it

Rejeição à inteligência artificial

A cibersegurança é a principal preocupação com a inteligência artificial (IA), revelou um inquérito em 17 países, embora 85% acredite que ela resulta numa série de benefícios. 61% dos inquiridos desconfia dos sistemas de IA e 67% tem uma "aceitação moderada". Outro inquérito de 2023 aponta os ciberataques como a maior preocupação para 80%, enquanto 78% a receia pelas capacidades de roubo de identidade e 74% que seja utilizada para criar anúncios políticos enganadores.



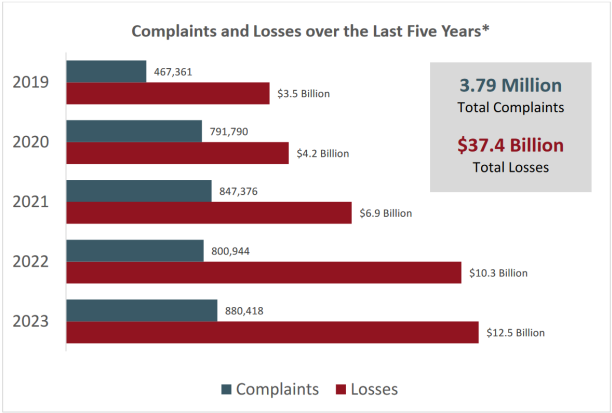
A vaia que a audiência do festival SXSW proporcionou este ano a conteúdos sobre a IA foi a mais recente demonstração de que nem todos estão satisfeitos com a evolução ou demonstram confiança na tecnologia. O Edelman Trust Barometer 2024 mostra resistência e entusiasmo com a IA, com 35% a rejeitá-la e 30% interessados na mesma. Tudo isto ocorre quando o Parlamento Europeu aprovou o AI Act.

Fontes: Trust in artificial intelligence: a global study; Public Trust in AI Technology Declines Amid Release of Consumer AI Tools; SXSW Audiences Loudly Boo Festival Videos Touting the Virtues of AI; Festival crowd boos San Francisco techies over 'AI is a culture' video; Edelman Trust Barometer; What You Need To Know About The EU AI Act

EUA: mais queixas ao FBI, mais roubos de identidade

O Internet Crime Report de 2023, publicado pelo Internet Crime Complaint Center (IC3) do FBI, revelou que os prejuízos com a cibercriminalidade atingiram os 12.500 milhões de dólares, relativos a cerca de 880 mil queixas – mais 10% do que em 2022.

Mais de 1.300 milhões de dólares foram perdidos em esquemas de roubo de identidade, com os criminosos a fazerem-se passar por autoridades do governo ou de suporte técnico. O número destas reclamações quase triplicou, crescendo de 13.633 em 2019 para 37.560 no ano passado.



Fontes: Internet Crime Report; Tech Support Firms Will Pay $26 Million to Settle FTC Charges That They Deceived Consumers into Buying Repair Services

BREVES

• Portugal tem "um grande potencial" para liderar em áreas como a IA, a cibersegurança ou a mobilidade sustentável, segundo a síntese do estudo "Megatendências 2050. O mundo em mudança. impactos em Portugal". O país "é e será um importante ponto de interesse para o mercado de dados", devido à localização geográfica estratégica entre a Europa e o Atlântico.

• Os ciberseguros normalizaram-se em muitas organizações, requerendo a atenção entre administradores financeiros (CFO), de TI (CISO), e apoio dos CEO.

• Como identificar um ciber-atacante, para efeitos legais ou outros, quando em muitos casos são apenas "programadores egoístas" a querer enganar todos, incluindo os seus pares.

• As recomendações da Agência de Segurança Nacional (NSA) para os CISO sobre a estratégia "zero-trust" no pilar Network and Environment devem ser adotadas por todas as organizações, nomeadamente para que "segmentem as redes e limitem o acesso de utilizadores não autorizados a informações sensíveis".

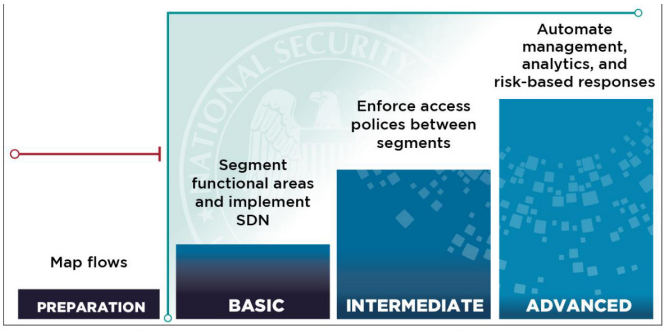


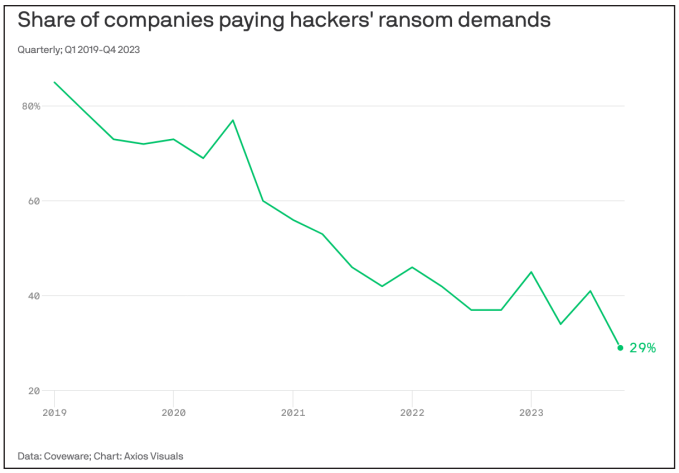
Figure 2: Zero Trust network and environment pillar maturity

• Iniciativas para software "open source" mais seguro.

• Visa gere meio milhão de ciberataques por mês.

• A França sofreu um ciberataque de "uma magnitude inédita, em intensidade, tempo e na desmultiplicação do número de pontos de ataque", com 800 sites sob pressão durante dois dias, declarou o ministro da Administração Pública, Stanislas Guerini.

• Numa atividade conhecida por "SubdoMailing", mais de 8.000 domínios e 13 mil subdomínios legítimos foram usados numa campanha de distribuição de spam e monetização de cliques.



• Deve-se ou não banir o pagamento dos (em queda) pedidos de ransomware? Os valores, normalmente em criptomoeda e, por vezes, duplicados com a repetição dos ataques após o pagamento, são elevados: o grupo LockBit acumulou mais de 125 milhões de dólares dos resgates nos últimos 18 meses.

• Lições do ciberataque à British Library.

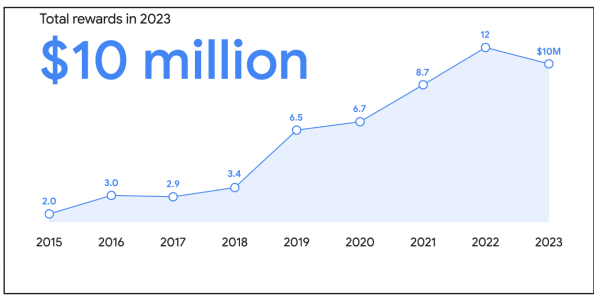
• Porque estão "red teams" a analisar modelos de IA? E porque são os assistentes de IA inseguros?

• Para agilizar tarefas comuns da cibersegurança, ChatGPT ou Gemini?

• A Microsoft vai lançar em Abril o "chatbot" de cibersegurança Copilot for Security, com um modelo de custo por "unidade de computação de segurança".

• O Microsoft Configuration Manager (MCM) ou System Center Configuration Manager (SCCM) é uma tecnologia usada por administradores de sistemas para gerir dispositivos em redes Windows, cujas fragilidades foram agora acumuladas por investigadores da empresa de "pen-testing" SpecterOps. A base de dados, Misconfiguration Manager, inclui ainda estratégias defensivas.

• No ano passado, a Google pagou 10 milhões de dólares a 632 investigadores de 68 países pela deteção e comunicação de falhas de segurança ("bug hunting") nos seus produtos e serviços.



• O National Cyber Security Centre britânico disponibilizou duas ferramentas online para analisar a segurança dos Web browsers (Check your web browser) e de validação da segurança do email (Check your email security), quando o roubo de passwords válidas tem aumentado para a distribuição de malware.

• O que é o software de segurança da informação e de gestão de eventos (SIEM) e como serve as necessidades das organizações.

• Recomendações para uma melhor gestão da segurança dos dados (SDM).

• O "problema invisível" no valor de 1.520 biliões de dólares do desajustado software antigo.

• O Cybercrime Atlas, uma colaboração público-privada internacional para mapear as relações entre grupos cibercriminosos e mitigar o impacto do cibercrime, deve entrar em funcionamento ainda este ano.

• O National Institute of Standards and Technology (NIST) norte-americano lançou a versão 2.0 do seu Cybersecurity Framework.

• A Federal Communications Commission aprovou o U.S. Cyber Trust Mark, um rótulo voluntário para indicar que dispositivos de consumo na Internet das Coisas (IoT) cumprem normas de cibersegurança. Estimativas apontam para mais de 1,5 mil milhões de ataques contra dispositivos IoT no primeiro semestre de 2021, cujo número deve ultrapassar os 25 mil milhões em funcionamento até 2030.

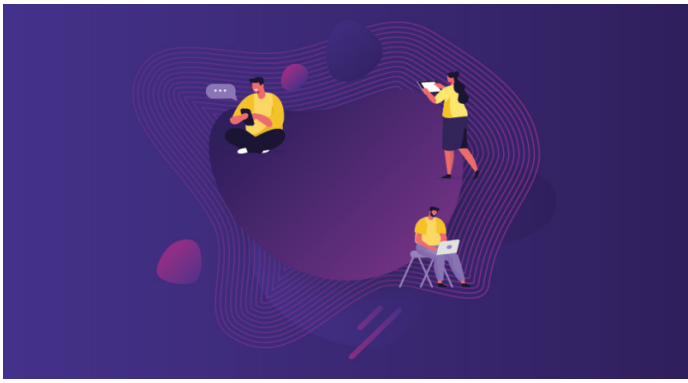
• Investigadores descobriram como incendiar um smartphone através do carregador sem fios.

A LER

Digital Services Act já é plenamente aplicável

Relatório sobre a cibersegurança e a resiliência das infraestruturas e redes de comunicações da EU

Comissão Europeia apresenta novas iniciativas para as infraestruturas digitais



Proteger as eleições na UE face aos desafios da cibersegurança

Alcançado acordo político sobre o Regulamento Cibersolidariedad

Cybersecurity for Beginners – a curriculum

Comissão lança convites à apresentação de propostas para investir mais de 176 milhões de euros em capacidades e tecnologias digitais

Back to the Building Blocks: A Path Toward Secure and Measurable Software

Diretora | Inês Esteves

Edição | Pedro Fonseca

Março 2024