ptsoc digest

julho 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

ptsoc digest
julho 2024

Grandes Opções 2024-28 antecipam revisão da Estratégia de Segurança do Ciberespaço

Imagem: Privecstasy, Unsplash

A proposta de Lei das Grandes Opções para 2024-2028 revela "que está proposta a revisão da Estratégia Nacional de Segurança do Ciberespaço 2019-2023" e que se pretende atribuir ao Centro Nacional de Cibersegurança (CNCS) "recursos adequados às necessidades presentes e futuras (desde logo, combater o cibercrime e as ameaças híbridas) e reforçar a sua cooperação com o Serviço de Informações de Segurança". Também o enquadramento jurídico da ciberperseguição, do ciberassédio ou do incitamento ao ódio online pode vir a ser revisto.

Segundo o documento, a cibersegurança é um "domínio que exige atenção redobrada, sendo fundamental apostar em sistemas de gestão da segurança de informação e dados, para proteger as pessoas e as empresas, mas também os órgãos e os serviços do Estado".

Fonte: Proposta de Lei

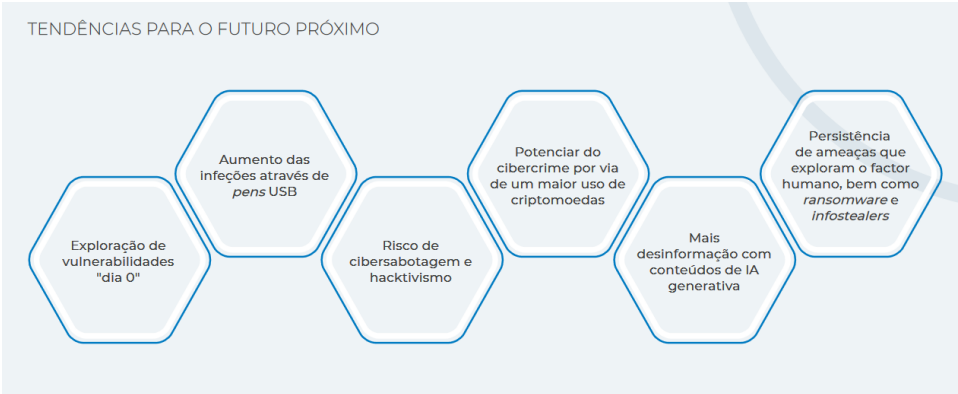
Ciberameaças olímpicas com resposta internacional

Os Jogos Olímpicos de Londres (2012) registaram mais de 212 milhões de ciberataques, número que subiu para 3.000 milhões nas Olimpíadas de Pequim em 2022. Desde Londres que estes eventos internacionais "se tornaram um campo de ensaio para os ciberataques, com pouco risco de retaliação".

Isso sucedeu com o Europeu de Futebol deste ano, um "prelúdio" ao que pode ocorrer nos Jogos Olímpicos em Paris, para os quais foram apresentadas algumas recomendações de segurança. As autoridades francesas vão ser ajudadas pelos EUA ou pela Estónia para se defenderem contra potenciais ciberataques, "à medida que aumentam as preocupações de que a Rússia possa tentar interferir" através de campanhas de desinformação.

Fontes: Computer Weekly, Stormshield, inCyber News, Dark Reading, Microsoft, Security Magazine (1,2)

Criminalidade informática aumentou em 2023, mas incidentes estabilizaram



Fonte: CNCS

O relatório Riscos e Conflitos do Observatório de Cibersegurança do CNCS aponta a existência de "uma perceção elevada de que aumentou o risco de uma entidade sofrer um incidente de cibersegurança no ciberespaço de interesse nacional em 2023 e 2024". O documento analisou os incidentes de cibersegurança e

do cibercrime no ano passado, e conclui que:

- a criminalidade informática aumentou mas o número de incidentes estabilizou nalguns indicadores;

- as ciberameaças mais relevantes foram o ransomware (nomeadamente na Administração Pública Local), o phishing e o smishing, outras formas de engenharia social, burlas online e comprometimento de contas;

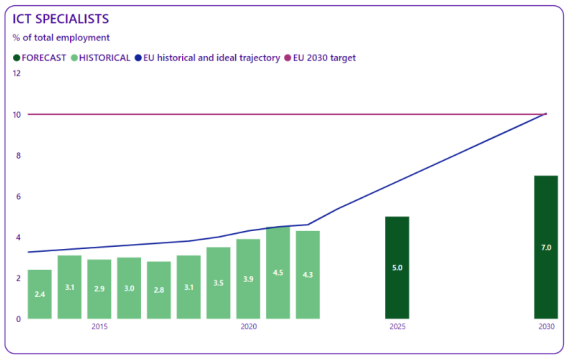
- cibercriminosos, atores estatais e hacktivistas são os principais agentes de ameaça, com os primeiros a liderar em número e impacto em serviços;

- os indivíduos e as PMEs foram as vítimas mais frequentes.

Fonte: Relatório Riscos & Conflitos

BREVES

ICT specialists



Note: The source of national forecast values is the 2023 country roadmap

Fonte: Digital Decade Country Report 2024

• Portugal terá falta de recursos humanos nas TIC, segundo o "Digital Decade 2024" da Comissão Europeia (CE), que apela ao reforço das competências em cibersegurança. Os números variam da escassez crítica dentro de dois anos - mitigada por novas estratégias para ter profissionais qualificados, nomeadamente ao diminuir a exclusão das mulheres num setor em que a falta de competências é "uma enorme fraqueza" - até quem defende que não existe falta de candidatos.

• A CE reconhece no mesmo relatório que as operadoras de em Portugal "estão a investir montantes significativos na substituição de equipamentos para cumprir os requisitos de segurança" no 5G, quando se sabe que os dispositivos móveis com esta tecnologia estão vulneráveis ao roubo de dados e ataques de negação de serviço. A ENISA abriu uma consulta pública para certificações 5G.

• O Instituto Politécnico de Beja ficou sem 50 mil euros num esquema de fraude informática conhecida por "CEO Fraud", semelhante ao que ocorreu com o Instituto de Gestão Financeira da Educação, mas em que as autoridades conseguiram recuperar os 2,5 milhões de euros transferidos para contas bancárias indevidas.

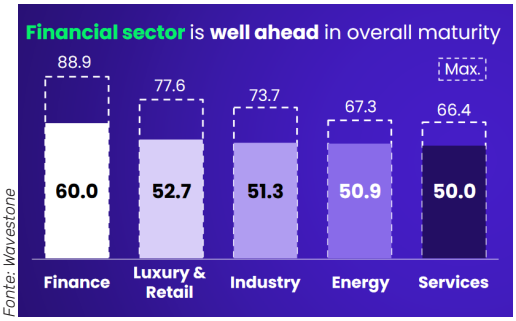
• Quase 700 queixas em Portugal pelo esquema Pig Butchering.

• A sofisticação e frequência dos ataques contra a cadeia de fornecimento de software está a aumentar e preocupa os profissionais de TI. Recentemente, foram divulgados dados pessoais de funcionários da Nokia e da Microsoft a partir do acesso a outras empresas, enquanto vulnerabilidades não detetadas deixaram aplicações macOS e iOS suscetíveis de incorporar código comprometido.

• O "complicado" papel da inteligência artificial (IA) na cibersegurança, quando a "corrida ao armamento" da IA divide os especialistas. Os CISOs devem planear estratégias para "disaster recovery" ou "ransomware recovery", e analisar o impacto nos recursos humanos. E o "AI hacking" não ficará limitado aos computadores.

• 78% das organizações vê a IA como um risco emergente mas mais de metade usa-a para melhorar a eficiência perante os riscos digitais. Estes aumentam com a estratégia de "Bring Your Own AI" para o local de trabalho.

• A OpenAI escondeu ter sofrido um ataque informático que pode ter "revelado segredos internos e suscitou preocupações em matéria de segurança nacional".



Fonte: Wavestone

• As grandes organizações aumentaram em 15% a força de trabalho dedicada à cibersegurança, com um profissional para cada 1.086 funcionários. Em 2023, um especialista lidava com 1.285 funcionários.

• Metade dos funcionários teme punição se comunicar erros de segurança dentro da sua organização.

• Os prémios a pagar pelos ciber-seguros estão a diminuir consoante melhora a cibersegurança nas organizações, mas o volume de sinistros continua a crescer e muitos ataques não estão "totalmente cobertos".

• Os ciberataques aumentaram em frequência e gravidade no último ano e a maioria das empresas não está preparada para ataques de ransomware, de phishing ou ao DNS.

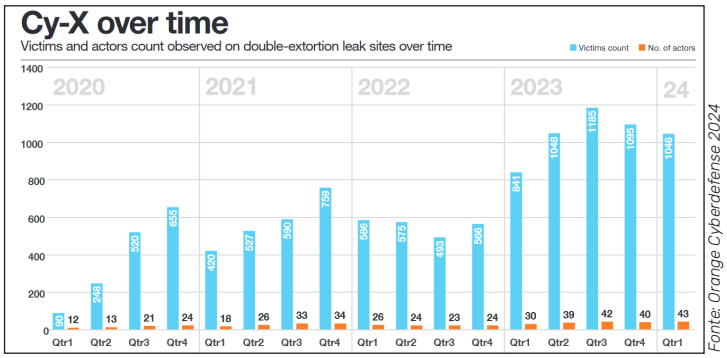
• Indústria automóvel preocupada com cibersegurança, quando ciberataques industriais fazem aumentar despesa em cibersegurança.

• Os deepfakes já chegaram ao mundo empresarial. Como os combater?

• "O impacto económico do ransomware é profundo, afetando empresas, governos e indivíduos a nível mundial. Compreender os fatores económicos que impulsionam o ransomware é crucial para desenvolver estratégias eficazes de combate a este flagelo crescente".

• Revitimização: uma nova tática dos grupos de ciberextorsão que, para isso, se estão a concentrar em táticas de evasão para "aumentar o tempo de permanência nas redes das vítimas".

• O valor médio dos pedidos de resgate em ataques de ransomware foi superior a 5 milhões de dólares no primeiro semestre de 2024. Aumento reflete confiança dos grupos criminosos nas suas capacidades e no valor dos dados roubados.



Fonte: Orange Cyberdefense 2024

• Os EUA não pretendem banir o pagamento dos ciber-resgates.

• Ministro das Comunicações da Indonésia pressionado a demitir-se na sequência de ciberataque com LockBit 3.0.

• Operadora sul-coreana de telecomunicações terá infetado com malware utilizadores de serviços P2P.

• Grupo de ransomware Volcano Demon usa chamadas telefónicas ameaçadoras para intimidar e negociar pagamentos com as vítimas.

• Lições sobre a "catástrofe" do ataque à Change Healthcare. A ordem executiva para analisar o "maior e mais sofisticado ataque" à SolarWinds não teve consequências.

• É melhor uma comunicação centralizada de ciberincidentes para "apoiar a transparência, a colaboração e a melhoria da segurança em todo o setor".

• O presidente da Microsoft prometeu mudanças na segurança dos produtos e serviços.

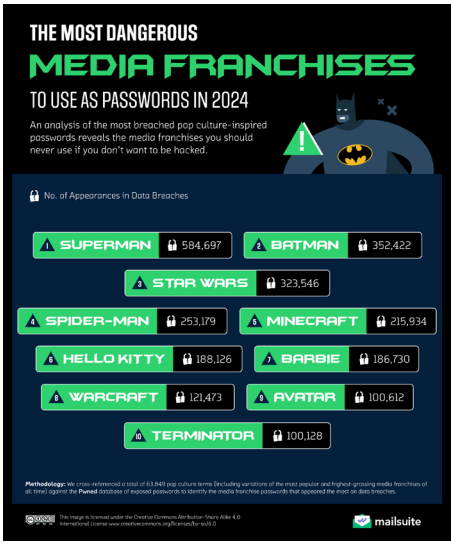
• O impacto da proibição norte-americana à empresa de cibersegurança Kaspersky.

• Ciberataque político nos EUA contra "think tank" conservador.

• 10 mil milhões de antigas e novas passwords divulgadas no ficheiro "RockYou2024".

• Violação de dados expôs registos de chamadas telefónicas e mensagens de texto de 110 milhões de clientes da operadora norte-americana AT&T, que terá pago pela eliminação dos dados mais sensíveis.

• 78% das pessoas usam a mesma password em diferentes contas. E quais são as passwords mais perigosas usando o nome de ícones culturais?



• Burlões enganam duplamente as vítimas com oferta de ajuda para recuperarem das burlas. Outros optam pela "intimidação física".

• Metade dos esquemas fraudulentos em Singapura ocorre em plataformas da Meta (WhatsApp, Facebook e Instagram). Em Macau, os ciberataques aumentaram em 2023 e continuam.

• Australiano acusado de criar pontos de acesso WiFi gratuitos a imitar redes legítimas, para captar dados pessoais.

• Apple alerta contra ataques de spyware nos iPhone, mas Android também é inseguro.

• Diretório de ferramentas e recursos de cibersegurança e ferramentas de análise de malware.

• Anos a encher a Web de conteúdos duvidosos.

A LER

Commission to invest over €210 million in cybersecurity, digital capacities and technology under the Digital Europe Programme.

State of the Cloud 2024: The Legacy Cloud is dead — long live AI Cloud!

Regulamento da Inteligência Artificial (versão final).

Regulamento do Parlamento Europeu e do Conselho que Cria Regras Harmonizadas em Matéria de Inteligência Artificial.

Calling Time on DNSSEC?

ESAs and ENISA sign a Memorandum of Understanding to strengthen cooperation and information exchange.

Diretora | Inês Esteves

Edição | Pedro Fonseca

Julho 2024