ptsoc digest

maio 2023

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

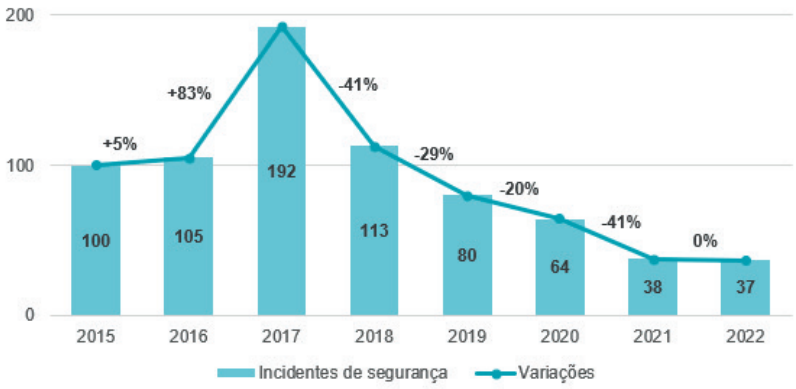
Registrars visitam Centro de Dados do PTSOC

Sete Registrars nacionais marcaram presença numa visita ao Centro de Dados e à sede do .PT, no início de Maio. O encontro com representantes da AMEN, Decimal, Domínios, PTisp, PTServidor, Webtech e WEBHS incluiu "flash talks" sobre os principais projetos em desenvolvimento: Inteligência Artificial na Gestão de Domínios, o Dados.PT, o PTSOC ou o Confio.pt.

Menos incidentes, mas com maior impacto

A entidade reguladora das comunicações, Anacom, foi notificada no ano passado de 37 incidentes de segurança pelas empresas de redes e serviços de comunicações eletrónicas. Apesar de manter a tendência decrescente dos últimos seis anos, com menos um incidente do que os registados em 2021, "o seu impacto, no entanto, foi muito assinalável, já que afetaram cerca de 6,4 milhões de assinantes, o que se traduz num aumento muito expressivo em relação a 2021".

Em fevereiro, um ataque "teve enorme impacto nas redes e serviços de um dos principais operadores de comunicações em Portugal, resultado de um ciberataque à sua rede core", e afetou as suas comunicações fixas e móveis a nível nacional. A distribuição geográfica dos incidentes é uniforme, com a região do litoral oeste continental a ter um maior número de incidentes, cuja duração média anual foi de 16 horas.



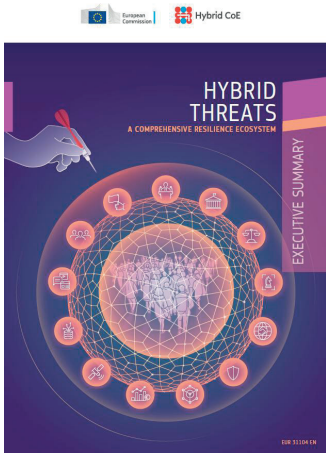
Fonte: Anacom

Governo cria Cyber Academia and Inovation Hub (CAIH)

O Governo aprovou em Conselho de Ministros a criação da Cyber Academia and Inovation Hub (CAIH), associação sem fins lucrativos para promover a formação, investigação, desenvolvimento e inovação no domínio do ciberespaço, bem como apoiar o desenvolvimento de capacidades no âmbito da sua interligação entre cibersegurança e ciberdefesa. Para "fomentar a convergência de interesses das indústrias, do tecido empresarial, e instituições de ensino superior com os organismos da Administração Pública, a Cyber Academia and Innovation Hub integra, para além da Defesa Nacional, entidades tuteladas por outras áreas governativas, nomeadamente, a Administração Interna; Justiça; Economia e Mar; Educação; Ciência Tecnologia e Ensino Superior e Digitalização e Modernização Administrativa".

Fonte: Conselho de Ministros

Cibersolidariedade e ameaças híbridas na UE



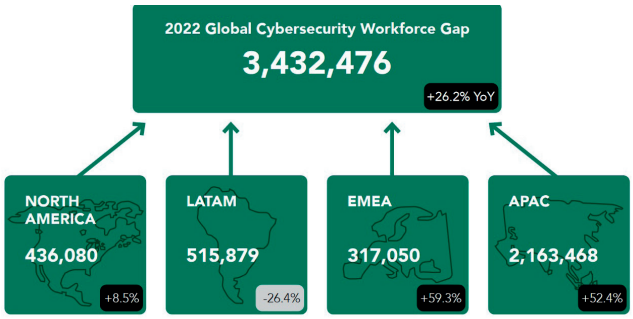
A Comissão Europeia adotou uma proposta de ato legislativo sobre cibersolidariedade (Cyber Solidarity Act), para reforçar as capacidades europeias na cibersegurança. Ele procura "tornar a Europa mais resiliente e mais reativa face às ciberameaças, reforçando simultaneamente o mecanismo de cooperação existente". Contribuirá para o desenvolvimento de um panorama digital seguro para os cidadãos e as empresas, bem como para proteger as entidades críticas e os serviços essenciais, como hospitais e serviços públicos. Uma análise aponta algumas preocupações sobre o Cyber Solidarity Act para o setor privado.

Em paralelo, o Centro Comum de Investigação da Comissão Europeia editou um novo relatório sobre as ameaças híbridas, uma combinação cada vez mais sofisticada de "diferentes tipos de instrumentos e ações organizadas, como a desinformação, a pressão económica, o abuso de migrantes, os ciberataques e outras ações encobertas".

Fontes: Comissão Europeia, Cyber Solidarity Act, Inside Privacy, Centro Comum de Investigação

Faltam recursos humanos na cibersegurança, nomeadamente mulheres

Os cortes orçamentais e os despedimentos de equipas de cibersegurança prosseguem enquanto aumentam as vulnerabilidades, ficando assim as organizações potencialmente mais vulneráveis a ataques. "A cibersegurança é uma profissão absolutamente crítica", mas esta tendência ocorre quando se alerta para o desinteresse das organizações e se estima que existam 3,4 milhões de empregos por preencher no setor da segurança informática. Para mais, esta escassez ocorre em paralelo com um "amplo desequilíbrio" em termos de género. Um estudo do (ISC)2 a mais de 11 mil trabalhadores nota que as mulheres com menos de 30 anos apenas representam 30% da força de trabalho, percentagem que cai para os 24% entre os 30 e 38 anos. "A diferença é ainda maior para as idades superiores a 39 anos, com a percentagem de mulheres na força de trabalho a atingir os 10%".



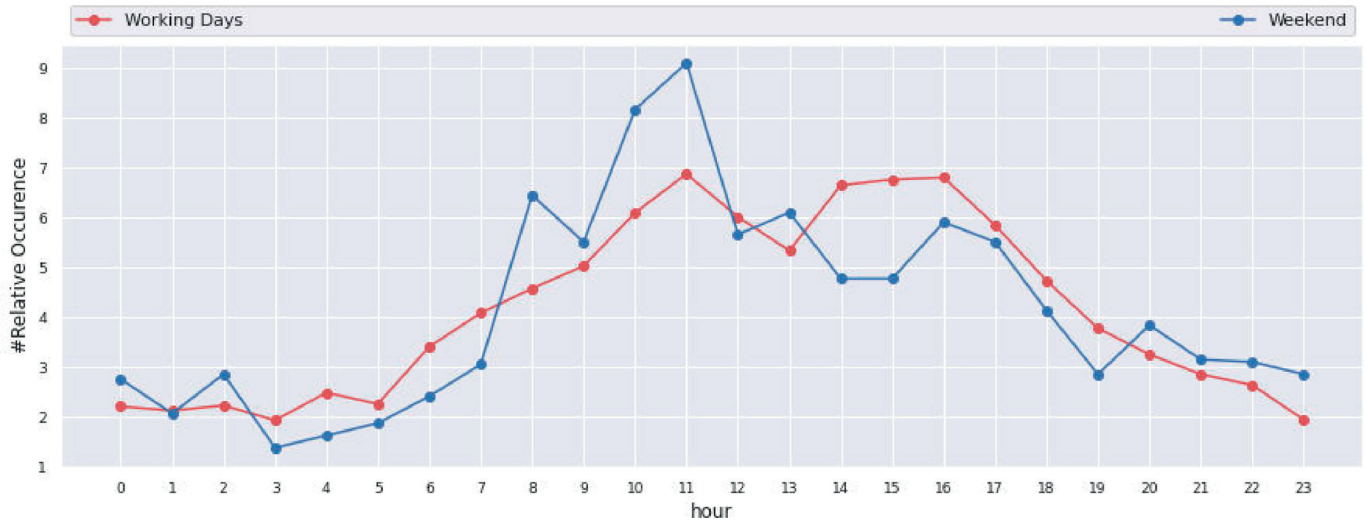
Fontes: HackerOne, WEF, Cybersecurity Dive, (ISC)2

35 anos depois, o mesmo problema

Uma nota do final de 2022, emitida pela NSA norte-americana, afirma que "cerca de 70% de todas as vulnerabilidades de segurança do software resultam de problemas de segurança da memória". Neste artigo, recorda-se que "o primeiro ataque informático amplamente destrutivo foi o Morris Worm em 1988, que explorou um problema na forma como os programas em C geriam a memória. 35 anos depois, o problema ainda não desapareceu, apesar da maioria das linguagens de programação que surgiram desde 1990 oferecerem algum tipo de segurança" nesse aspeto.

Fontes: NSA, O'Reilly, Morris Worm

Phishing na epidemia? Em horário das 9 às 5…



Investigadores holandeses analisaram mais de 500 mil mensagens electrónicas de phishing enviadas para 1.100 diferentes domínios nos Países Baixos. As conclusões do estudo refletem que "a maioria das mensagens eletrónicas de phishing relacionadas com a COVID-19 seguem padrões conhecidos, o que indica que é mais provável que os autores se adaptem do que reinventem os seus esquemas". Os investigadores confirmaram ainda conhecimentos anteriores "sobre padrões temporais, como o facto de a maioria dos emails de phishing serem recebidos no horário de trabalho durante a semana".

Fonte: Computers & Security

Perspetivas para gerir mentalidades na cibersegurança

Quando 52% dos CISOs nos EUA e Reino Unido não conseguem proteger totalmente os segredos das suas organizações, sete orientações para manter uma atitude positiva:

1. A segurança é um destino
2. A segurança é detida pelos profissionais
3. A segurança está a tornar-se cada vez mais difícil
4. A segurança é um produto
5. A segurança é impulsionada pelo crime
6. A segurança é 100% alcançável
7. A segurança é ingrata

Fonte: GitGuardian, CSO

Breves

• O CNCS publicou "Tecnologias Emergentes", uma visão sobre cloud computing, Internet das Coisas, Inteligência Artificial, tecnologia móvel 5G e tecnologias quânticas.

• O National Cyber Security Centre do Reino Unido alertou para a "ciberproliferação" de ferramentas e serviços comerciais para ciberataques.

• O estado do cibercrime no primeiro trimestre de 2023.

• As cinco novas técnicas de ciberataques mais perigosas.

• As principais tendências nas ciberameaças, segundo a Gartner.

• Sete conselhos para ajudar as organizações a evitarem alguns ataques.

• No atual panorama da resolução de crises de segurança, tanto atacantes como defensores estão a acelerar o ritmo.

Figure 1: Top Threat Groups for Ransomware-as-a-Service Ecosystem

Source: Halcyon (March 2023)

• Ransomware Malicious Quadrant, para ranking de grupos.

• Novas táticas para assegurar o pagamento de ransomware, que já chegou à indústria musical.

• Empresas da cibersegurança industrial criaram a Emerging THreat Open Sharing (ETHOS), uma plataforma de alertas para partilha de informações sobre ameaças.

• A ENISA publicou uma avaliação das normas para a cibersegurança da inteligência artificial (IA), com recomendações para as futuras políticas da UE nesta matéria.

• A desinformação é o novo malware? E a Dark Web a maior ciberameaça?

• A China tem 50 hackers por cada ciberagente do FBI, diz o diretor da agência norte-americana.

• A primeira versão do Tratado da ONU sobre o Cibercrime será publicada em Junho, com preocupação sobre o que o documento poderá abranger.

• A Google obteve uma ordem judicial temporária nos EUA para interromper a distribuição do malware CryptBot e "desacelerar" o seu crescimento que, só em 2022, atingiu mais de 670 mil computadores. Também o Departamento de Justiça dos EUA confiscou os domínios de 13 serviços "DDoS-for-hire".

• Autoridades ucranianas prenderam um homem por vender dados de mais de 300 milhões de pessoas de diferentes países.

• BellaCiao: o mais recente malware iraniano

• Cibercriminosos aproveitam interesse na IA para disseminar malware.

• Boas práticas criptográficas.

• "Bélgica legaliza o hacking ético: uma ameaça ou uma oportunidade para a cibersegurança"?

• No rasto de Dark Avenger: o programador de vírus mais perigoso do mundo

• Como os cibercriminosos foram enganados por uns alegados telemóveis para comunicações cifradas.

• Milhões de smartphones Android pré-infetados com malware.

• No mundo do "car hacking", os ladrões de carros usam tecnologia disfarçada em velhos telemóveis Nokia e colunas Bluetooth.

• O aumento dos preços globais dos ciberseguros foi moderado no primeiro trimestre de 2023, com preços médios a crescerem apenas 11%, por comparação com os 28% do trimestre anterior.

• ICANN com novo projeto Inferential Analysis of Maliciously Registered Domains (INFERMAL) para analisar ciberataques e possíveis medidas de mitigação nos domínios de topo (TLD).

• Super Mario Bros. pirateado distribui malware. Nada de novo, mas NCSC britânico lançou campanha de sensibilização para jovens.

Diretora | Inês Esteves

Edição | Pedro Fonseca

maio 2023