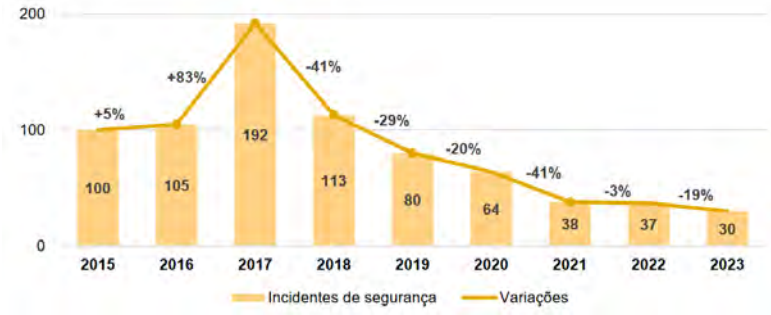
ptsoc digest

maio 2024

Diretora | Inês Esteves • Edição | Pedro Fonseca

.pt ptsoc Centro de Operações de Segurança

ANACOM recebeu 30 notificações em 2023



Unidade: número de incidentes de segurança
Fonte: ANACOM

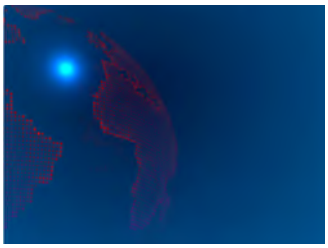
A ANACOM recebeu no ano passado um total de 30 incidentes de segurança, o "volume mais baixo de ocorrências desde 2015" (com uma média anual de 84 casos).

Apesar do número mais reduzido destas notificações obrigatórias das empresas de redes e serviços de comunicações eletrónicas, a entidade reguladora nota que "o seu impacto foi superior ao registado no ano anterior, uma vez que foram afetados 6,9 milhões de assinantes, mais 7% do que em 2022. Para este acréscimo contribuiu a ocorrência de um incidente, em dezembro, que envolveu a interligação de voz de dois dos principais operadores de comunicações em Portugal, com impacto no serviço de telefonia móvel".

Num outro caso, uma operadora sofreu um ataque de ransomware sem "impacto significativo". Das 30 notificações, apenas em 10 foi prestada informação ao público, como sucedeu recentemente com a Equinix.

Fontes: Anacom, Público ($)

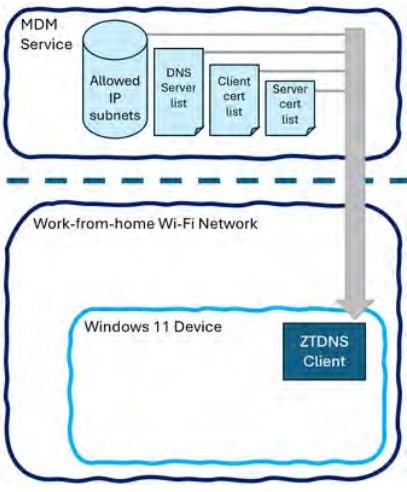
LLM contra Dark Web



O Atlantic Security Award 2024 foi entregue a Alexandra Mendes, do Departamento de Engenharia Informática da Faculdade de Engenharia da Universidade do Porto (FEUP), pelo projeto "Leveraging Large Language Models Trained on Dark Web Data to Support Decision Making for Atlantic Security and Defense". Este procura desenvolver "um modelo que facilite a formulação de políticas, estratégias e políticas de defesa, e operações das forças de segurança contra o cibercrime, comércio ilícito, e outras ameaças facilitadas pela Dark Web no Atlântico".

Fonte: FLAD

Microsoft mais segura



Antecipando-se a uma possível responsabilização das empresas de tecnologia nos EUA, a segurança é agora uma "prioridade de topo" para a Microsoft, após ter sido criticada pelas suas práticas neste âmbito – nomeadamente por vender a segurança como uma oferta "premium". Esta prioridade está também associada a uma compensação para os responsáveis da empresa, cujo presidente Brad Smith deve ser ouvido no House Homeland Security Committee.

Entretanto, a empresa anunciou o desenvolvimento do Zero Trust DNS (ZTDNS) para versões futuras do Windows, procurando conseguir uma maior segurança nos acessos de dispositivos a endereços de rede fiáveis.

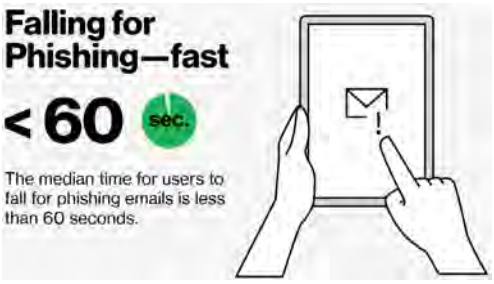
Fontes: Cybersecurity Dive (1, 2), The Verge (1, 2), Ars Technica, Axios, Directions on Microsoft, The Register, Politico, Microsoft

BREVES

• Como se mede o sucesso na cibersegurança?

• Espanha: o regresso dos Caretos, uma centena de detenções por esquema no WhatsApp do "filho em apuros" e 30 pessoas presas pelo método "man in the middle", que também afetou utilizadores em Portugal.

• O encerramento pelas autoridades (incluindo a Polícia Judiciária) da plataforma de "phishing-as-a-service" LabHost, usada por 10 mil utilizadores (nomeadamente jovens universitários), levou à prisão de 37 suspeitos e à desativação de 40 mil domínios.



• O "2024 Data Breach Investigations Report" da Verizon revela novas linhas de ciberataques ou razões para o aumento de vulnerabilidades, e como o "elemento humano" é uma das principais causas nas violações de segurança.

• BogusBazaar: numa das "maiores fraudes de sempre", o grupo criminoso criou mais de 75 mil sites com promessas de desconto em conhecidas marcas de luxo.

• Os prolíficos e perigosos burlões do grupo "Yahoo Boy" gerem dezenas de esquemas fraudulentos nas redes sociais.

• Paris prepara-se para os ciberataques durante os Jogos Olímpicos.

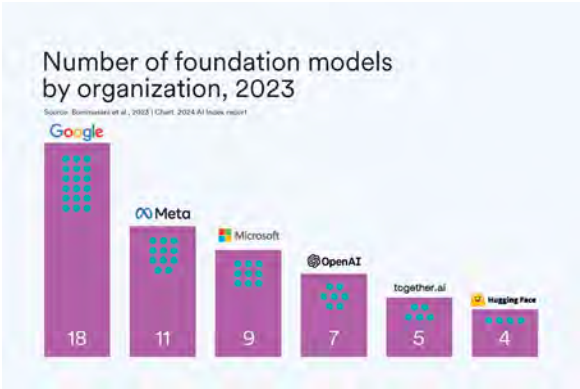
• A ENISA não vai criar uma base de dados de vulnerabilidades. Nos EUA, sistemas semelhantes (a Common Vulnerabilities and Exposures Records e a National Vulnerability Database) estão a ser criticados.

• A NATO vai estabelecer um Integrated Cyber Centre (NICC) para agilizar "a colaboração entre peritos civis, profissionais da indústria, pessoal militar e o corpo político" da organização no domínio da ciberdefesa.

• 50% da Web é tráfego automatizado por "bots", embora nos últimos 12 meses possa não ter passado dos 29% e "nem todos são maus".

• Estratégias para uma cadeia de fornecimento segura de software.

• Apesar do "estado da inteligência artificial" (IA) ainda poder ser "prejudicial, não fiável e estar a ficar sem dados", as empresas estão a investir em sistemas de IA generativa (GenAI) para "transformar grandes questões de segurança em ações concretas, ajudar nas operações de segurança e, cada vez mais, tomar medidas automatizadas".



• Num "espaço imaturo" como o das certificações em IA nas áreas da governança e da cibersegurança, vale a pena investir no "complexo industrial das certificações"?

• Questões de segurança que devem integrar qualquer política de uso aceitável da IA.

• Investigadores usaram a IA para detetar o branqueamento de capitais com bitcoins.

• Uma década de ransomware, o "State of Ransomware 2024", a proliferação de ferramentas para este tipo de ataques e como ativar a proteção contra ransomware no Windows.

• Das 1750 organizações alertadas pela Cybersecurity and Infrastructure Security Agency (CISA) norte-americana para vulnerabilidades de ransomware, "apenas metade agiu".

• O "sucesso" do grupo Scattered Spider nos ataques de ransomware deve-se a serem "especialistas em engenharia social" e "fluentes na cultura ocidental".

• O site de ransomware do LockBit voltou a ser encerrado pelas autoridades e revelada a identidade do alegado administrador do grupo.

• Desde 2023, os responsáveis pelo ransomware Akira receberam 42 milhões de dólares de 250 vítimas.

• O CEO da UnitedHealth pagou um ciber-resgate de 22 milhões de dólares.

• O Reino Unido adotou as primeiras leis para proteger consumidores e organizações contra pirataria informática e uso de nomes de utilizador e passwords fracas.

• A descoberta de passwords "demora agora mais tempo do que no passado, mas isso não é motivo de comemoração".

• O ecossistema do "open source" precisa de uma segurança mais rigorosa para os colaboradores?

• Maioria dos ataques a PME visam vulnerabilidades com mais de cinco anos.

• Seis maus hábitos que tornam as PME em alvos fáceis e cinco questões que os líderes das organizações não devem ignorar na cibersegurança.

• Hacktivistas exploram falhas nos fornecedores de infra-estruturas críticas. Autoridades querem mais segurança nessas organizações.

• Um grupo de ciberespionagem ligado ao Irão usa falsas identidades de ativistas ou de jornalistas para campanhas de engenharia social.

• O United Nations Development Programme (UNDP) sofreu um ataque de ransomware, com roubo de dados internos, o Parlamento Europeu alertou para um acesso indevido à sua aplicação usada no recrutamento de pessoal temporário e o grupo IntelBroker assumiu um ataque à Europol.

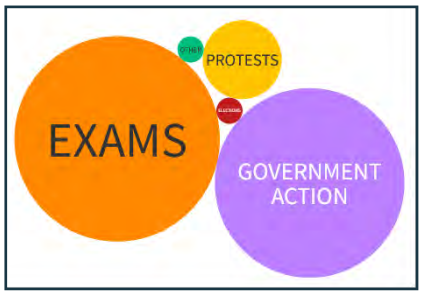
• A insegurança das caixas de comentários.

• Identificadores físicos e comportamentais para a autenticação biométrica.

• Identificação humana vs. não-humana em SaaS e gestão de identidades com "identity fabric immunity" ou com "identity and access management".

• À procura dos dados perdidos com ferramentas de "data security posture management" (DSPM).

• Ameaça às redes: demonstração de um ataque em seis passos.



• Países do Médio Oriente e Norte de África desligam, "repetidamente e sem justificação", a Internet nas épocas dos exames escolares. E nos EUA?

• Algumas ferramentas de "pen-testing", que atravessa uma "era dourada".

• Como funciona um ataque de "vishing".

• Os pêndulos que protegem a Internet.

• Será que os utilizadores adotaram as passwords reveladas nos filmes?

• Jogo para aprender a proteger-se de um ataque de ransomware.

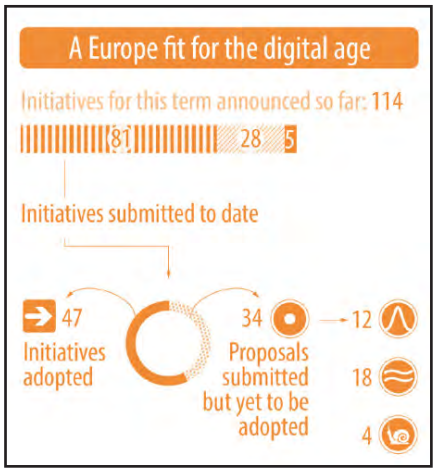
A LER

Cyber Resilience Act Requirements Standards Mapping

Shaping Cybersecurity Policy towards a trusted and secure Europe

Informal meetings of EU27 ministers on infrastructure security and consumer protection

The six policy priorities of the von der Leyen Commission: An end-of-term assessment



United States International Cyberspace & Digital Policy Strategy

2024 Report on the Cybersecurity Posture of the United States

Deploying AI Systems Securely - Best Practices for Deploying Secure and Resilient AI Systems

AI Risk Management Framework

What's happened to my data?

The cybersecurity of fairy tales

Diretora | Inês Esteves

Edição | Pedro Fonseca

Maio 2024