IT Insight SECURITY

#28 FEVEREIRO 2026

ZERO TRUST PARA LÁ DO HYPE

360

Security & Compliance

Transforme a gestão da segurança e conformidade da sua organização com uma solução integrada e modular, que oferece visibilidade e controlo total, em tempo real.

Saiba mais ▸

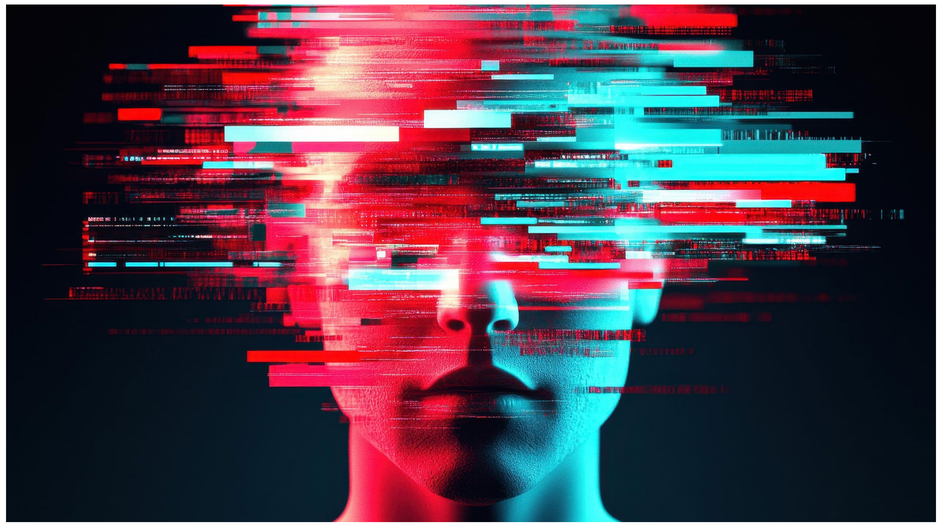
claranet® | 360 Security & Compliance

BROWSE

COVER

BRAVE NEW WORLD

▼ DEEPFAKE DETECTION & SYNTHETIC IDENTITY FRAUD



BLUE TEAM

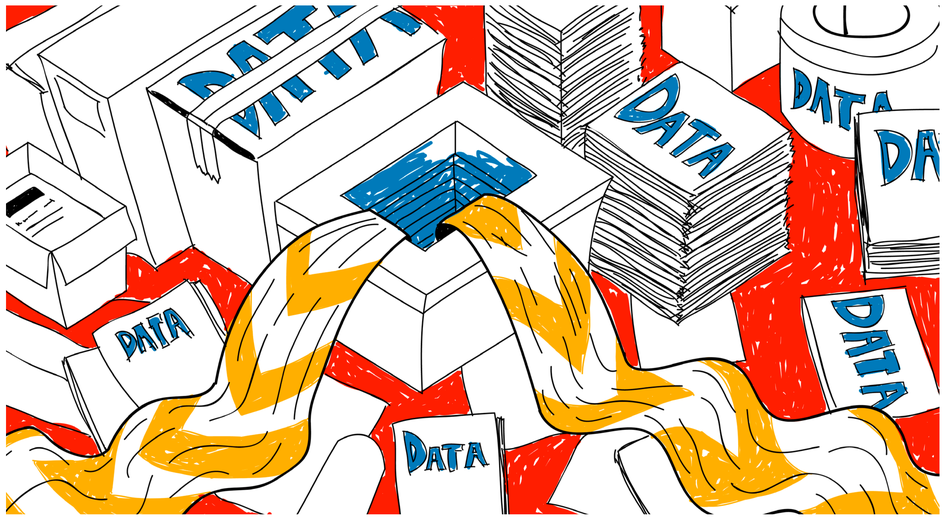
▼ ACCENTURE

ANCHOR

▶ HENRIQUE CARREIRO

RISK

▼ DATA ACT



EXPERT

▼ OLIVIA ARANTES INCM

▼ TERESA PEREIRA, CYBER THREAT HUNTER

▼ FERNANDO AMORIM, CIIWA

Security & Networking ReAImagined

Proteja e acelere dados na cloud e IA, em qualquer lugar.

A cloud e a Inteligência Artificial revolucionaram a forma como trabalhamos. Foi por isso que criámos a Netskope e é também por isso que mais de 30% das empresas da Fortune 100 confiam em nós.

A Netskope nasceu para a era da cloud e da IA.

Com a Netskope, cloud, dados, IA, dispositivos e redes são protegidos de forma contínua, permitindo às organizações defenderem-se ativamente contra ameaças em constante evolução.

Não criámos apenas uma plataforma. Criámos a base para a próxima geração de negócios seguros e de alto desempenho.

Descubra o que nos move.

netskope

netskope.com

S.LABS

claranet®

Cibersegurança na era dos deepfakes: proteger a confiança

cso chief security officers

Zero Trust: From Buzzword to Real Implementation

CYBER INSPECT

A identificação de risco como base da Cibersegurança

netskope

Como construir um modelo Zero Trust num mundo de LLM

PROLOGIN PRODUTOS E SERVIÇOS

"NIS 2: Da conformidade legal à resiliência estratégica – O caminho para a maturidade digital"

...e ainda

SECURNET ALWAYS ONLINE | ALWAYS SECURE

S.LABS

O S.Lab ou Security Labs é um espaço de criação e partilha dentro da IT Security, onde exploramos e desenvolvemos ideias em colaboração com os nossos parceiros. Aqui, transformamos conceitos em conteúdos relevantes e envolventes, seja através de artigos, vídeos, webinars, podcasts ou conferências. O nosso objetivo é dar forma a ideias que não cabem nos formatos tradicionais, criando novas formas de comunicar e inovar.

cso
chief security officers

O EQUILÍBRIO ENTRE A DISPONIBILIDADE E O RISCO É A CHAVE PARA A SEGURANÇA DA INFORMAÇÃO

CONHECIMENTO - ÉTICA - RIGOR

www.cso.pt | info@cso.pt

PRONTOS OU NÃO, AÍ VEM A NIS2

RUI DAMIÃO

O mês de dezembro trouxe, por fim, a publicação em Diário da República da NIS2, ou Decreto-Lei n.º 125/2025. 120 dias depois da publicação, ou seja, a 3 de abril deste ano, o Decreto-Lei entra em vigor. O momento que se esperava há já alguns anos chegou e as organizações já não têm desculpas: agora é preciso tratar de estar *compliant* com a NIS2.

A diretiva europeia não é uma *checklist*; as organizações devem-na tratar como um ponto de partida para melhorar a cibersegurança dos seus processos, das suas pessoas e da sua tecnologia.

Um dos pontos de grande importância da diretiva prende-se com o Artigo 28.º do Decreto-Lei nacional. Segundo este artigo, as organizações devem considerar "os aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos".

Se as grandes e médias empresas estão, de uma maneira geral, minimamente prontas para a NIS2 e viradas para os temas de cibersegurança, as pequenas empresas (que compõem grande parte do tecido empresarial) não só não estão, como nem sempre têm os recursos financeiros para fazer os investimentos necessários.

Assim, as organizações mais pequenas têm – se ainda não o fizeram – de começar a utilizar aquilo que já é considerado como básico em cibersegurança, mas que nem sempre é feito: autenticação multifator, *backups* regulares e testados, segmentação de rede, atualizações dos sistemas operativos e aplicações, mas também formação regular de colaboradores, um inventário de ativos e um plano de resposta a incidentes, entre muitas outras coisas. O objetivo é sempre o mesmo: melhorar a proteção do ciberespaço como um todo.

Os ciberataques em Portugal não vão terminar no dia 3 de abril; nos dias 4, 5, 6 e por aí fora vão continuar a existir. Mas, pela primeira vez, há consequências reais (financeiras, legais e pessoais) para quem ignorar o problema. Se isso não chega para mudar comportamentos (e se calhar não chega), nada vai mudar. ◀

PROLOGIN
PRODUTOS E SERVIÇOS

Mordeu o isco?

A PROLogin protege a sua empresa contra as armadilhas digitais. Somos especialistas em IT e cibersegurança, com soluções completas para manter os seus dados e sistemas a salvo.

A cibersegurança não vive de alarmismos, mas de ação contínua
Visite prologin.pt e fale connosco.

www.prologin.pt
(+351) 214 261 699
(Chamada para a rede fixa nacional)
@prologin_pt

HENRIQUE CARREIRO

IA: DOS DADOS ENVENENADOS AOS MODELOS COMPROMETIDOS

Há um pressuposto tácito na adoção acelerada de modelos de IA generativa: o de que um modelo é mais um componente de software – complexo, mas um componente. Mas o seu comportamento não é escrito em código; é destilado a partir de dados. Se a integridade desses dados falha, falha a integridade do próprio sistema – e a falha pode permanecer latente, à espera de um gatilho (*trigger*).

O envenenamento de dados (*data poisoning*) é precisamente isso: a introdução deliberada de exemplos maliciosos no pré-treino dos modelos, no *fine-tuning* ou até no *corpus* que alimenta *embeddings*, para induzir vieses, degradação seletiva ou *backdoors* acionados por frases específicas. Em outubro de 2025, um estudo conjunto do UK AI Security Institute, da Anthropic e do Alan Turing Institute mostrou que bastaram 250 documentos maliciosos para inserir um *backdoor* em modelos entre 600M e 13B parâmetros; no *setup* descrito, esses 250 documentos (cerca de 420 mil tokens) representaram aproximadamente 0,00016% do total de tokens de treino.

Este detalhe altera a economia do ataque. Em vez de "controlar uma percentagem" do *corpus*, um adversário pode plantar poucas sementes em locais bem escolhidos: conteúdo público preparado para ser recolhido, contributos em *datasets* de instruções obtidos por *crowd-sourcing*, ou uma fase de afinação conduzida por um fornecedor. Trabalhos de investigação recentes sobre envenenamento durante o *instruction tuning* descrevem como gatilhos discretos podem ser aprendidos, ainda que preservando a aparência "limpa" do conteúdo, tornando a deteção por filtragem e inspeção superficial pouco fiável. Esta fiabilidade é corroída por uma assimetria fundamental: a injeção é estatisticamente invisível nos agregados de dados (não altera médias nem variâncias) e é semanticamente camuflada para revisores humanos. Tratam-se de ataques *clean-label*: o texto lê-se como legítimo para o revisor, mas carrega a lógica tóxica para a máquina. Onde o filtro vê sintaxe válida, o modelo vê uma instrução imperativa oculta.

O problema, a prazo, é sistémico. Treinamos modelos sobre cadeias longas (web, fornecedores, *logs* internos); afinamos com *datasets* reaproveitados; e colocamo-los a produzir texto e código que regressam ao ecossistema digital. A superfície de ataque vai-se acumulando: o mesmo veneno pode reaparecer por reutilização de *corpora*, por *transfer learning* e por "modelos derivados". Uma alteração pequena, mas persistente, tende a sobreviver aos ciclos de atualização.

O risco mais sério surge quando um *backdoor* se manifesta num contexto operacional. Pode não aparecer em testes de aceitação nem em avaliações genéricas; pode emergir apenas quando a frase certa entra num e-mail, num ticket ou numa página web lida por um agente. Em SOC, em *pipelines* de DevSecOps assistidos por IA, ou em triagens automatizadas, isso transforma o envenenamento num problema de cadeia de fornecimento, com impacto na disponibilidade e, sobretudo, na integridade das decisões. O cenário torna-se crítico pela ausência de reversibilidade. Ao contrário do software, onde uma vulnerabilidade se resolve com um *patch*, não existe um método limpo para fazer uma rede neuronal "desaprender" um conceito sem degradar as suas capacidades gerais (*catastrophic forgetting*). A descoberta tardia de um *backdoor* não exige apenas uma correção; exige, frequentemente, o descarte do modelo e o custo proibitivo de um treino integral.

As respostas defensivas convergem para uma conclusão pragmática: tratar dados como infraestrutura crítica. As orientações conjuntas da CISA/NSA/FBI recomendam práticas clássicas — prova de proveniência, assinaturas digitais, cifragem, controlo de acesso, armazenamento seguro, e rastreio da cadeia de fornecimento — aplicadas ao ciclo de vida dos dados usados para treinar e operar modelos de IA generativa. O Reino Unido está a traduzir princípios semelhantes para um código de prática que cobre o ciclo de vida de sistemas de IA, do desenho ao fim de vida.

Se houver uma crise, ela não virá de um "modelo rebelde", mas de uma rastreabilidade deficiente daquilo que o alimentou. A maturidade mede-se menos em *benchmarks* e mais em perguntas simples: de onde veio cada *dataset*, quem o tocou, que transformações sofreu, que sinais de adulteração foram procurados, e que testes de *backdoor* foram feitos antes de o pôr em produção. Estes são, daqui para a frente, os dados fulcrais que esperamos no *model card* de cada modelo, independentemente de qual o fornecedor. Não se trata de exigência esotérica: é higiene básica. ◀

SECURNET

ALWAYS ONLINE | ALWAYS SECURE

MAIS DO QUE UMA MARCA, UM PARCEIRO DE CONFIANÇA.

☆☆ **HPE FY'24**	Parceiro do Ano - HPE GreenLake Parceiro do Ano - HPE Aruba Networking
☆ **Veeam Software**	The best COM partner of the year 2024
☆☆ **IT Channel Award'25**	Parceiro Cybersecurity Parceiro do Ano
☆☆ **Best Portuguese Partner Award** (IGNITION)	Sealpath partner of the year 2025 AlgoSec partner of the year 2025
☆ **Splunk'25**	Parceiro do Ano em "Novos Clientes"

A TECNOLOGIA EVOLUI. E NÓS TAMBÉM.

PORTO +351 224 673 094
LISBOA +351 213 622 204

BASE EUROPEIA DE VULNERABILIDADES ENTRA EM OPERAÇÃO

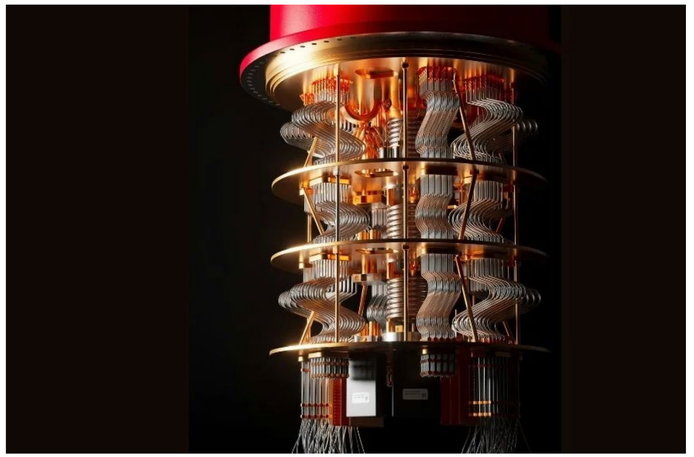
Nova base de dados pública da GCVE aposta num modelo descentralizado para reforçar a soberania digital europeia e reduzir a dependência de plataformas norte-americanas.

A Europa passou a dispor de uma nova base de dados pública de vulnerabilidades de segurança informática. A db.gcve.eu, lançada pela iniciativa GCVE – Global Cybersecurity Vulnerability Enumeration, já está operacional e pretende oferecer uma alternativa aberta e descentralizada aos sistemas tradicionais de catalogação de falhas de segurança, como o CVE, largamente utilizado a nível global.

O lançamento surge na sequência das preocupações levantadas em 2025 com a possibilidade de descontinuação do programa Common Vulnerabilities and Exposures (CVE), um cenário que expôs a dependência do ecossistema europeu de infraestruturas críticas sediadas nos Estados Unidos. Esse episódio funcionou como catalisador para a criação de soluções alternativas focadas na autonomia e resiliência digital. ◀

RELATÓRIO DA EUROPOL DEFINE MIGRAÇÃO PARA CRIPTOGRAFIA PÓS-QUÂNTICA

Um relatório conjunto da Europol propõe uma abordagem prática para a adoção de criptografia pós-quântica no setor financeiro, face aos riscos futuros da computação quântica.



Um novo relatório conjunto da Europol e dos seus parceiros apresenta um enquadramento estruturado para apoiar instituições financeiras na preparação da migração para criptografia pós-quântica, num contexto em que os avanços da computação quântica ameaçam a robustez dos atuais métodos de encriptação.

Intitulado "*Prioritising Post-Quantum Cryptography Migration Activities in Financial Services*", o documento visa apoiar as organizações na transição do planeamento estratégico para a execução prática.

A metodologia assenta na avaliação de fatores como a sensibilidade dos dados protegidos, o tempo de vida esperado dessa informação, o nível de exposição a potenciais atacantes e o impacto para o negócio em caso de comprometimento. ◀

CYBER INSPECT

PROTEJA OS SEUS CLIENTES E TRANSFORME CIBER RISCOS EM OPORTUNIDADES DE NEGÓCIO

A CyberInspect é uma plataforma de testes de cibersegurança orientada para prestadores de serviços de IT e cibersegurança, que permite identificar riscos digitais em escala, em empresas e organizações, contribuindo para reduzir a sua exposição a ciberameaças.

Saiba mais

A IDENTIFICAÇÃO DE RISCO COMO BASE DA CIBERSEGURANÇA

NUM CONTEXTO DE RISCO CRESCENTE, A CYBERINSPECT POSICIONA A IDENTIFICAÇÃO DE VULNERABILIDADES COMO O PONTO DE PARTIDA PARA UMA CIBERSEGURANÇA MAIS EFICAZ E ALINHADA COM A REALIDADE DAS EMPRESAS.

O aumento da exposição digital tem vindo a colocar a cibersegurança no centro das decisões empresariais. Em Portugal, os ciberataques cresceram 36% em 2024 e, em 2025, 54% das empresas foram alvo de pelo menos um incidente. Estes números refletem uma realidade em que o risco deixou de ser excecional para passar a ser estrutural, fruto do aumento da superfície de ataque das empresas, provocada pela digitalização dos negócios e a dependência crescente de serviços digitais.

As pequenas e médias empresas (PME) são particularmente afetadas. A limitação de recursos, a ausência de equipas dedicadas e a dificuldade em acompanhar a evolução das ameaças contribuem para níveis de maturidade mais baixos. Em 2025, 48% das PME portuguesas foram alvo de ciberataques com recurso a Inteligência Artificial, uma tendência alinhada com o contexto europeu, onde 43% das PME reportaram incidentes nos últimos dois anos.

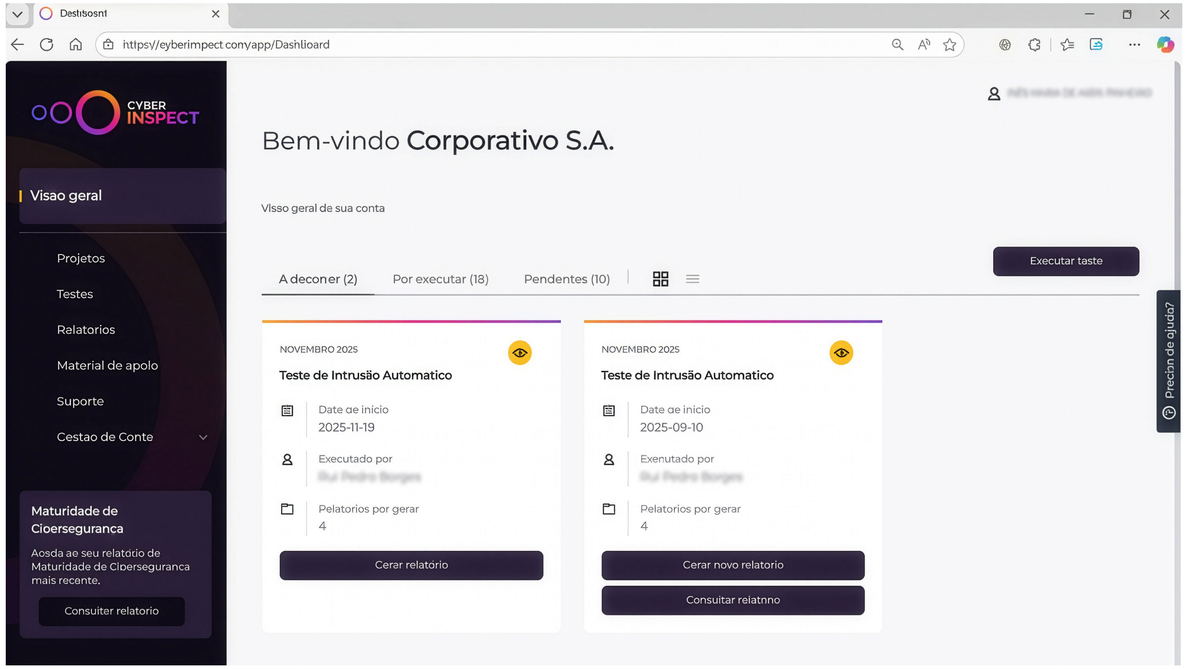
Para estas organizações, a falta de visibilidade sobre riscos e vulnerabilidades continua a ser um dos principais obstáculos à adoção de uma estratégia de cibersegurança eficaz.

PORQUE A IDENTIFICAÇÃO DE RISCO É A BASE DA CIBERSEGURANÇA

Antes de investir em tecnologias ou serviços de segurança, é essencial compreender onde estão os riscos reais. A identificação de risco permite mapear ativos, detetar vulnerabilidades e avaliar o impacto potencial de uma exploração, criando uma base objetiva para a definição de prioridades. Sem este diagnóstico, as organizações tendem a adotar abordagens genéricas ou reativas, com retorno limitado.

Num contexto em que os ambientes empresariais estão em constante mudança, avaliações pontuais deixaram de ser suficientes. A adoção de Cloud, a exposição crescente a serviços digitais e a sofisticação das ameaças exigem avaliações contínuas, estruturadas e acionáveis. A identificação de risco deixa, assim, de ser apenas um exercício técnico para se tornar um instrumento de apoio à decisão, tanto ao nível operacional como estratégico.

Os prestadores de serviços de IT e cibersegurança desempenham aqui um papel determinante. São o primeiro ponto de contacto das PME e beneficiam de uma relação de confiança já estabelecida. No entanto, para responder de forma eficaz, necessitam de ferramentas que lhes permitam avaliar riscos de forma simples, escalável e consistente, sem comprometer a produtividade das equipas.



UMA ABORDAGEM ESTRUTURADA À AVALIAÇÃO DE RISCO NAS EMPRESAS

É neste contexto que a **CyberInspect** se afirma como uma plataforma orientada para prestadores de serviços IT e Managed Services, que procuram estruturar e escalar ofertas de avaliação de risco junto da sua base de clientes. Lançada pela NOS em 2025, a *CyberInspect* permite integrar testes de cibersegurança no portefólio de serviços de forma simples e automatizada, criando uma base objetiva para serviços de remediação, compliance e acompanhamento contínuo do risco.

NUM CENÁRIO EM QUE O RISCO É CRESCENTE E INEVITÁVEL, A IDENTIFICAÇÃO ESTRUTURADA DE VULNERABILIDADES É O PONTO DE PARTIDA PARA UMA CIBERSEGURANÇA EFICAZ. A CYBERINSPECT ASSUME ESSE PAPEL COMO BASE DE UMA ABORDAGEM MAIS CLARA, CONTÍNUA E ALINHADA COM A REALIDADE DAS EMPRESAS

Através de um único ponto de acesso, a plataforma CyberInspect agrega diferentes serviços de avaliação de risco que permitem aos prestadores de serviços estruturar e escalar ofertas de cibersegurança junto dos seus clientes.

A plataforma inclui um índice de risco de cibersegurança para análises iniciais e comparação com o mercado, testes de intrusão automáticos que replicam técnicas reais de ataque, mapeamento contínuo de vulnerabilidades com base em catálogos de referência atualizados diariamente, bem como análise de código e questionários de avaliação da maturidade de cibersegurança.

Esta abordagem integrada facilita a identificação de prioridades e suporta a transição do diagnóstico para serviços de remediação.

Cada avaliação gera um relatório técnico detalhado, com vulnerabilidades identificadas e recomendações de mitigação. Complementarmente, a plataforma disponibiliza um **Smart Report**, desenvolvido pela CyberInspect com recurso a Inteligência Artificial, que consolida os resultados de diferentes testes e destaca, de forma clara, as correções mais críticas a priorizar. Este modelo facilita a comunicação com decisores e acelera a transição do diagnóstico para a ação.

DA IDENTIFICAÇÃO DE RISCO À CRIAÇÃO DE VALOR NOS SERVIÇOS DE CIBERSEGURANÇA

Concebida para prestadores de serviços IT e de cibersegurança, a CyberInspect funciona como uma base para estruturar e escalar ofertas de avaliação de risco. Ao simplificar a execução dos testes e a interpretação dos resultados, a plataforma reduz barreiras técnicas e operacionais, permitindo transformar a identificação de vulnerabilidades em serviços de maior valor acrescentado, como remediação e acompanhamento contínuo, num contexto de crescente exigência do mercado.

Num cenário em que o risco é crescente e inevitável, a identificação estruturada de vulnerabilidades é o ponto de partida para uma cibersegurança eficaz. A CyberInspect assume esse papel como base de uma abordagem mais clara, contínua e alinhada com a realidade das empresas.

AVALIE O SEU RISCO DIGITAL DOS SEUS CLIENTES

Conheça a CyberInspect e perceba como a identificação estruturada de risco pode apoiar uma estratégia de cibersegurança mais eficaz nas empresas.

Explore a plataforma CyberInspect ◀

IT·SECURITY SUMMIT PORTO 2026 APRIL

#A VOZ DOS CISO

14 ABRIL 2026 | GAIA

TIVOLI KOPKE PORTO GAIA

A VOZ DOS CISO

Depois do sucesso da primeira edição, a IT Security Summit regressa à região Norte com uma ambição reforçada, duplicando o espaço em plateia para acomodar um número ainda maior de leitores da revista IT Security e profissionais do setor, respondendo ao crescente interesse e relevância do evento na região.

Centrada nos temas da resiliência e compliance com ênfase nas necessidades práticas das empresas da região norte e dando voz aos seus protagonistas, a IT Security Summit será uma oportunidade para explorar as tecnologias mais inovadoras que impactam um grande número de indústrias, para além da partilha de conhecimentos entre CISO, CSO, diretores de segurança e diretores de IT com responsabilidade de cibersegurança, originando um ecossistema único de networking.

INSCREVA-SE AQUI!

por Victor Andrade, CEO, PROLogin

“NIS 2: DA CONFORMIDADE LEGAL À RESILIÊNCIA ESTRATÉGICA – O CAMINHO PARA A MATURIDADE DIGITAL”

A ENTRADA EM VIGOR DA DIRETIVA NIS 2 REPRESENTA UMA MUDANÇA ESTRUTURAL NA FORMA COMO AS ORGANIZAÇÕES EUROPEIAS — E, EM PARTICULAR, AS PORTUGUESAS — ENCARAM A CIBERSEGURANÇA.

Num contexto de ameaça cada vez mais sofisticado, persistente e profissionalizado, a segurança da informação deixou definitivamente de ser um tema exclusivamente técnico para se afirmar como uma **prioridade estratégica ao mais alto nível da gestão**.

Hoje, a conformidade já não é um ponto de chegada. É um processo contínuo de governação do risco, proteção de ativos críticos e garantia da continuidade do negócio.

UM NOVO PARADIGMA DE RESPONSABILIDADE

Ao contrário da sua antecessora, a NIS 2 não se limita a recomendar boas práticas. Introduz **obrigações claras, impacto operacional direto e responsabilidade explícita da gestão de topo**. A diretiva exige uma abordagem estruturada, mensurável e transversal à organização, onde a gestão de risco, a resiliência operacional e a capacidade de resposta a incidentes assumem um papel central.

Para os CISO e IT Managers, esta mudança traduz-se numa realidade incontornável: a cibersegurança passa a ser tão crítica para a sustentabilidade do negócio como a gestão financeira, a cadeia logística ou a conformidade regulatória. Soluções pontuais, silos tecnológicos ou abordagens reativas deixam de ser suficientes — e aceitáveis.

DA EXIGÊNCIA LEGAL À EXECUÇÃO OPERACIONAL

Na prática, a NIS 2 impõe a adoção de um conjunto robusto de medidas técnicas e organizacionais: monitorização contínua, gestão proativa de vulnerabilidades, controlo rigoroso de acessos, proteção avançada de endpoints, planos

sólidos de continuidade de negócio e, de forma particularmente relevante, **gestão do risco na cadeia de abastecimento**.

Acrescem ainda prazos de notificação de incidentes extremamente exigentes e um nível de escrutínio regulatório sem precedentes. Num cenário em que minutos podem fazer a diferença entre um incidente controlado e uma crise com impacto financeiro, operacional e reputacional, o mercado exige **estratégias integradas, auditáveis e comprovadamente eficazes**.

PROLOGIN E SOPHOS: DA ESTRATÉGIA À AÇÃO

É neste contexto que a PROLogin assume um papel de parceiro estratégico. Com mais de uma década de experiência em cibersegurança e IT em Portugal, e como **Parceiro Platinum da Sophos**, ajudamos as organizações a transformar os requisitos da NIS 2 em capacidades reais, alinhadas com a sua maturidade digital e com os seus objetivos de negócio.

Mais do que implementar tecnologia, atuamos como um verdadeiro **braço direito do CISO**, garantindo que a segurança reforça a confiança, acelera a tomada de decisão e sustenta o crescimento da organização.

TECNOLOGIA COMO CATALISADOR DA RESILIÊNCIA

O ecossistema de soluções Sophos, implementado e gerido pela equipa da PROLogin, permite responder de forma direta e integrada aos principais pilares da NIS 2, através de uma abordagem orientada à **prevenção, deteção e resposta**.

Soluções como Endpoint Protection, XDR e MDR garantem visibilidade contínua e capacidade de resposta rápida a incidentes. O serviço de **Managed Detection and Response (MDR)** destaca-se como um fator crítico de sucesso, oferecendo vigilância 24/7 por equipas especializadas — uma capacidade que poucas organizações conseguem sustentar internamente — e assegurando que ameaças são neutralizadas antes de escalarem para incidentes graves.

Complementarmente, tecnologias como **Next-Generation Firewall, Email Security e Zero Trust Network Access (ZTNA)** reduzem drasticamente a superfície de ataque e asseguram que o acesso a dados críticos é feito de forma controlada, segura e totalmente auditável.

Esta **visibilidade end-to-end do ambiente de IT** não só mitiga riscos reais, como permite demonstrar conformidade regulatória de forma clara, estruturada e defensável perante as autoridades.

NIS 2 COMO VANTAGEM COMPETITIVA

Em conjunto, a PROLogin e a Sophos ajudam as organizações a **reduzir risco, aumentar a resiliência operacional e acelerar a maturidade digital**. Quando bem abordada, a NIS 2 deixa de ser um exercício burocrático e passa a ser uma **oportunidade estratégica** para reforçar a postura de segurança, ganhar eficiência operacional e preparar o futuro.

Num mundo digital interligado, a confiança é o ativo mais valioso de uma organização. Investir em cibersegurança madura é proteger o património, salvaguardar a continuidade do negócio e criar bases sólidas para um crescimento sustentável.

Hoje, a cibersegurança não é apenas um requisito legal — é o **alicerce sobre o qual se constrói o sucesso de amanhã**. ◀




Cibersegurança

IT Insight talks

25 de fevereiro | Forum Tecnologico Lispólis | 10h00

A primeira IT Insight Talk de 2026 é dedicada à **Cibersegurança** e realiza-se no Fórum Tecnológico Lispolis, em Lisboa, onde exploraremos as complexidades e desafios em constante mudança do mundo da cibersegurança. Para além da mesa-redonda habitual, contará com 2 keynotes de abertura a não perder.
2026 acrescenta uma mudança substancial ao formato habitual, que passará a ser integralmente transmitido via zoom, logo a partir das 10h00. Este evento híbrido proporcionará aos participantes oportunidades de networking e uma experiência imersiva e interativa, oferecendo insights valiosos e práticas fundamentais para proteger dados e sistemas críticos num mundo digital em constante mudança.

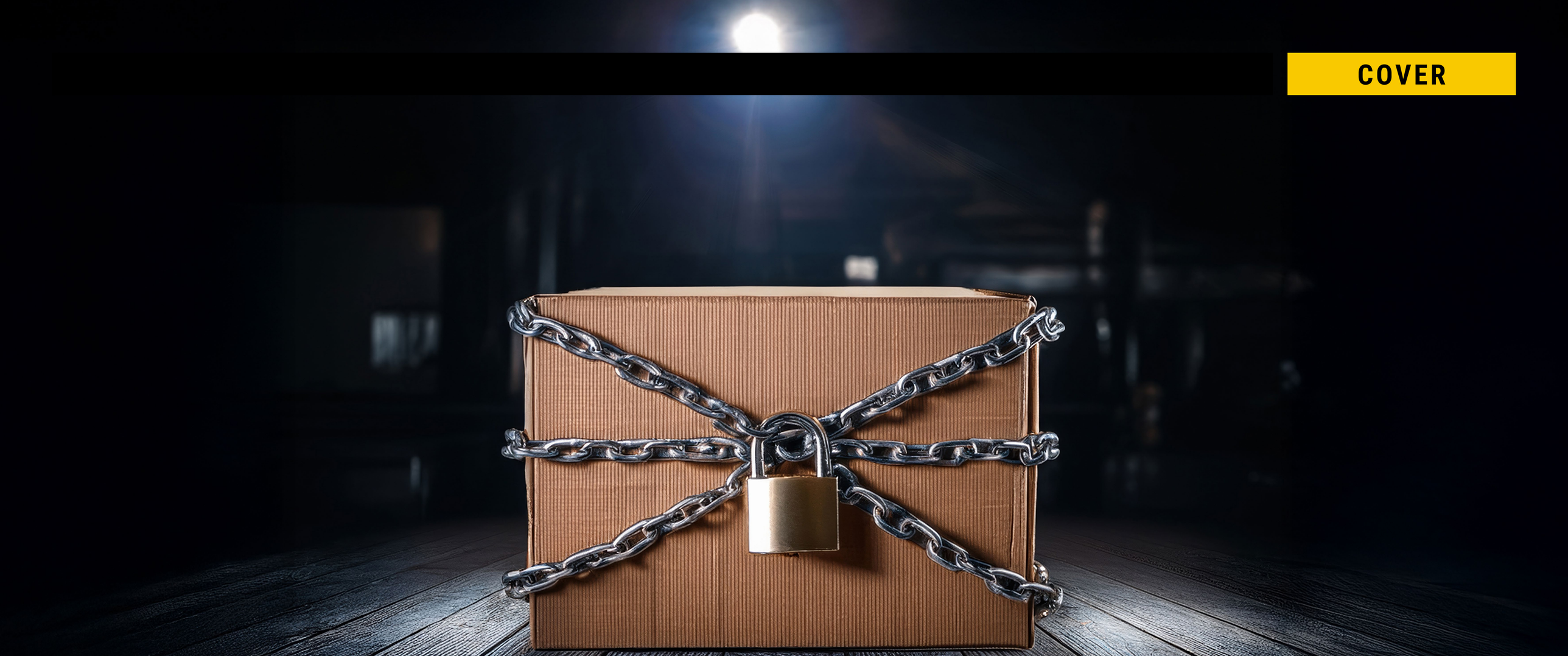
Junte-se a nós no próximo dia 25 de fevereiro, no Fórum Tecnológico de Lisboa, a partir das 9h30
Escolha a sua forma de participar:

QUERO ESTAR PRESENTE **QUERO ASSISTIR POR ZOOM**

Patrocinado por: cybersafe, LOGICALIS Architects of Change, ManageEngine, SECURNET ALWAYS ONLINE | ALWAYS SECURE, Symantec by Broadcom, VisionWare since 2005

Com o apoio de: LISPOLIS PÓLO TECNOLÓGICO DE LISBOA

COVER



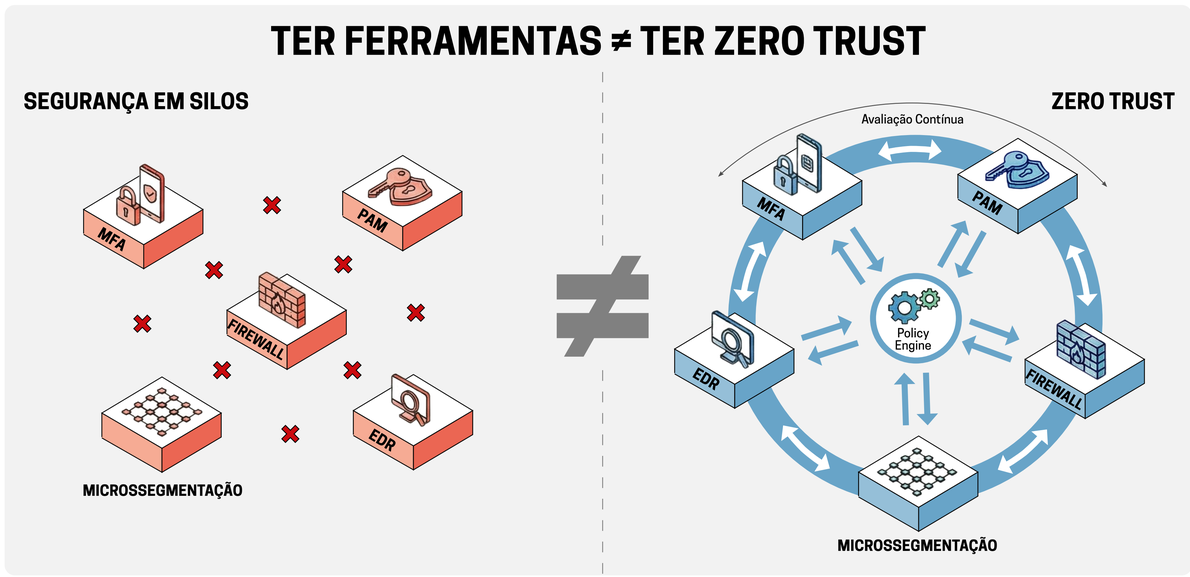
ZERO TRUST NÃO VEM NUMA CAIXA; VEM COM RESISTÊNCIA INTERNA

POR RUI DAMIÃO

O MERCADO PROMETE ZERO TRUST COMO SOLUÇÃO TECNOLÓGICA, MAS A REALIDADE É DIFERENTE. ESTIMA-SE QUE APENAS 10% DAS GRANDES EMPRESAS VENHAM A TER UM PROGRAMA DE ZERO TRUST MADURO ATÉ 2026; OS RESTANTES 90% VÃO DESCOBRIR QUE O VERDADEIRO OBSTÁCULO NÃO ESTÁ NA TECNOLOGIA.

O mercado de segurança zero trust movimentou 36,96 mil milhões de dólares em 2024 e projeta-se que atinja os 92,42 mil milhões até 2030, segundo a Grand View Researh. Os números refletem uma transformação profunda, mas entre o *hype* do mercado e a realidade da implementação, existe um território onde muitos projetos morrem ou ficam reduzidos a implementações cosméticas.

David Grave, Security Director da Claranet Portugal, defende que "ter ferramentas isoladas é segurança em silos, não é zero trust" e indica que "o que falta é a orquestração política unificada e a avaliação contínua de contexto". Assim, a chave está na palavra "*trust*": a confiança não pode ser estática, tem de ser reavaliada a cada pedido.



Pedro Soares, National Security Officer da Microsoft Portugal, concorda que os componentes como MFA, microssegmentação e PAM "cobrem alguns pilares, mas não representam uma implementação completa". O modelo "é holístico e parte do princípio de que nenhum acesso é confiável por defeito".

Já Ricardo Marciano, Business Development Manager SASE da Fortinet, aponta que "estamos a falar de controlos isolados em silos que não comunicam entre si nem alimentam decisões de acesso em tempo real".

Manfred Ferreira, Business Developer Manager de Cyber Security & Network da Noesis, enquadra a questão numa perspetiva mais ampla: o foco do CISO deve ser equilibrado entre múltiplos pilares, desde iniciativas estratégicas à governação corporativa, passando pelo cumprimento regulatório e pela gestão do risco. "A adoção de MFA, microssegmentação ou PAM são medidas fundamentais. No entanto, estas iniciativas, por si só, não constituem a aplicação integral do modelo zero trust".

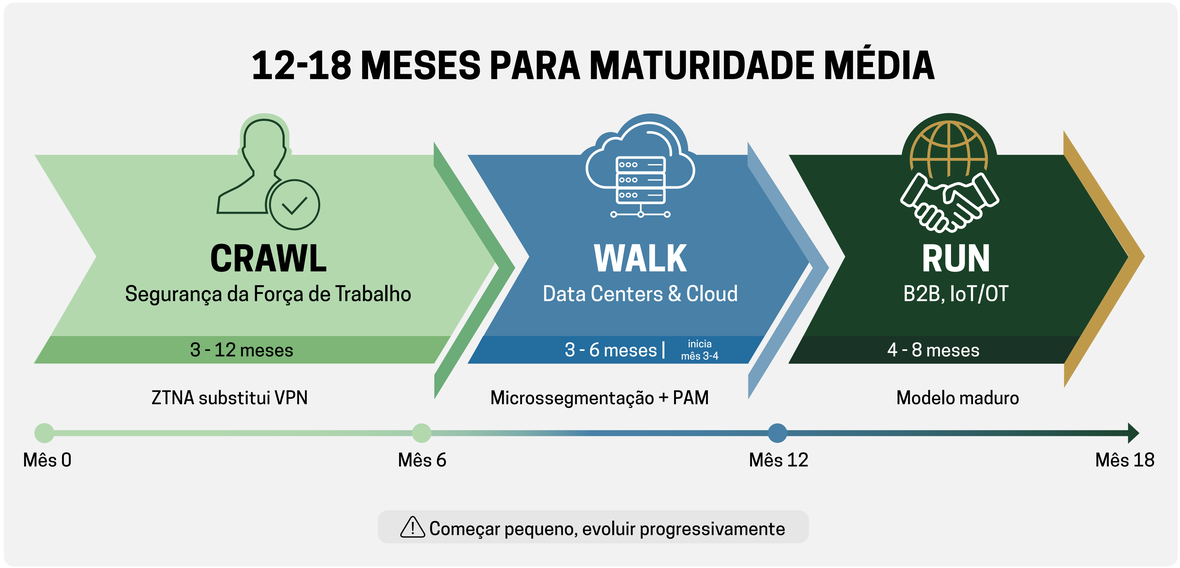
DAVID GRAVE, CLARANET PORTUGAL

PARA LÁ DA CHECKLIST

A Gartner estima que, até 2026, apenas 10% das grandes empresas vão ter um programa zero trust maduro e mensurável, uma subida face a menos de 1% em 2022.

Quando questionados sobre os componentes técnicos não negociáveis, os especialistas convergem: identidade forte e centralizada com capacidade de integrar sinais de risco em tempo real, avaliação de postura do dispositivo com telemetria contínua

> "SE UM ATACANTE ROUBAR AS CREDENCIAIS DE UM ADMINISTRADOR, CONSEGUE MOVER-SE LATERALMENTE SEM SER DETETADO DURANTE QUANTO TEMPO? O ACESSO É REVOGADO AUTOMATICAMENTE? SE A RESPOSTA É NÃO, ENTÃO NÃO É ZERO TRUST"
>
> DAVID GRAVE, SECURITY DIRECTOR DA CLARANET PORTUGAL



e EDR/MDR integrado e *enforcement* granular através de Zero Trust Network Access (ZTNA) ou microssegmentação.

David Grave sublinha a importância da orquestração. "Se um atacante roubar as credenciais de um administrador, consegue mover-se lateralmente sem ser detetado durante quanto tempo? O acesso é revogado automaticamente? Se a resposta é não, então não é zero trust". Ricardo Marciano alerta que "sem identidade como plano de controlo central, o zero trust transforma-se apenas numa versão mais sofisticada de controlo do perímetro".

Pedro Soares diz que "sem estes três elementos não há mínimo viável" e que "seria como tentar montar um banco com uma perna a menos". Manfred Ferreira adota uma perspetiva mais abrangente, recusando limitar a abordagem. Assim, para além dos pilares iniciais, como acessos internos, SASE para externos e DLP, defende uma evolução transversal que abranja gestão de vulnerabilidades, governação de IA e quantificação do risco em impacto financeiro.

QUANDO O ZERO TRUST FALHA

O erro mais comum, segundo David Grave, é "tentar implementar zero trust na rede antes de mapear as aplicações". É fácil bloquear tráfego lateral com base em suposições teóricas, mas aplicações *legacy* críticas param por dependências não documentadas. "A falha não é tecnológica; é de visibilidade". Assim, "primeiro monitorizamos em modo *audit only* para descobrir o mapa real de tráfego; só depois aplicamos o *deny all*".

Com base numa situação que acompanhou, o representante da Claranet Portugal menciona que os sistemas *legacy* foram retirados "temporariamente" do zero trust, mas quando o sistema entrou em produção, os técnicos continuaram a usar acessos *legacy* nunca removidos. Numa auditoria, detetaram que 40% dos acessos não passavam pelo PEP. "O zero trust existia, mas não era *enforced* na realidade".

Pedro Soares partilha um caso de uma empresa que comprou um pacote completo sem faseamento: "uma *micro-segmentation appliance* para a rede, um sistema de ZTNA para substituir VPN e integração com a plataforma de IAM corporativa". A expectativa foi alta, com um investimento significativo, diz. O projeto foi planeado para 12 meses, mas falhou na execução e adoção. "A equipa aplicou políticas muito restritivas inicialmente e, de repente, aplicações legítimas começaram a falhar", explica. Ao desligar a VPN antiga, por exemplo, os utilizadores ficaram sem acesso a aplicações durante dias "até se criar uma exceção emergencial". "Quando as queixas chegaram ao nível executivo, ficou claro que o projeto estava a falhar e que, apesar de se ter gastado o dinheiro nas ferramentas, muitas delas não estavam de facto em uso efetivo. Grande parte do software caro tornou-se *shelfware*", afirma.

Para Manfred Ferreira, há um padrão de fundo. "O sucesso do zero trust está diretamente relacionado com o nível de expectativa, preparação e alinhamento para a sua adoção". Quando não é concedido tempo necessário para interiorizar a dimensão e impacto, os efeitos são claros: "atrasos na execução, decisões tardias, repetição de discussões, menor cobertura face ao potencial esperado". Este cenário pode gerar resistência e transições ruidosas.

PEDRO SOARES, MICROSOFT PORTUGAL

As lições passam pela implementação faseada com pilotos, mapear dependências previamente e criar uma equipa multidisciplinar com governança definida. Ricardo Marciano assume que as "organizações que começam por ZTNA sem maturidade em

> A RESISTÊNCIA "MANIFESTA-SE EM ATRASOS, FALTA DE PRIORIDADE OU EXCEÇÕES EM EXCESSO". QUANDO NÃO É BEM COMUNICADO, "É PERCEBIDO COMO ENTRAVE, GERANDO RESISTÊNCIA INFORMAL: COLABORADORES CONTORNAM POLÍTICAS, USAM DISPOSITIVOS PESSOAIS, GUARDAM DOCUMENTOS LOCALMENTE"
>
> PEDRO SOARES, NATIONAL SECURITY OFFICER DA MICROSOFT PORTUGAL

identidade e catalogação de aplicações enfrentam fricção excessiva e pressão para exceções" e, muitas vezes, "o erro não é tecnológico, mas de sequência e *governance*".

O OBSTÁCULO ORGANIZACIONAL

Um estudo da StrongDM de novembro de 2024 revelou que 48% dos profissionais de segurança apontam restrições de custo e recursos como o maior desafio, enquanto 22% reportam resistência interna.

David Grave identifica as equipas que construíram carreiras a gerir perímetros, firewalls e VPN como um obstáculo, uma vez que o "zero trust exige redefinir totalmente o modelo mental de 'rede interna de confiança' que estas equipas dominam há décadas". Também destaca resistência de administradores seniores habituados a "acesso total". "É preciso convencer que os '*super-admins*' também precisam de acesso '*just-in-time*'", diz.

Ricardo Marciano aponta "fragmentação da responsabilidade" como um obstáculo organizacional. "A identidade pertence a uma equipa, *endpoints* a outra, rede a outra. O zero trust exige decisões transversais e isso expõe zonas cinzentas de *ownership*", explica. Assim, o bloqueio manifesta-se como resistência passiva: adiamentos, exceções constantes, narrativa de que "o negócio não está preparado".

RICARDO MARCIANO, FORTINET

Pedro Soares observa que a resistência "manifesta-se em atrasos, falta de prioridade ou exceções em excesso". Quando não é bem comunicado, "é percebido como entrave, gerando resistência informal:

> "ZERO TRUST NÃO DEVE SER VISTO COMO RESULTADO, MAS PRÁTICA CONTÍNUA. QUEM ENTRA À ESPERA DE CHEGAR AO FIM DESISTE RAPIDAMENTE E QUEM ENTRA PARA EVOLUIR COLHE RESULTADOS REAIS"
>
> RICARDO MARCIANO, BUSINESS DEVELOPMENT MANAGER SASE DA FORTINET

colaboradores contornam políticas, usam dispositivos pessoais, guardam documentos localmente". Manfred Ferreira sublinha que a transição "trata-se de uma transformação organizacional que deve ser *top-down*".

CUSTO REAL E ARQUITETURA

Para uma empresa portuguesa entre 500 e mil colaboradores, Pedro Soares estima um *total cost of ownership* entre os 600 mil e os 800 mil euros ao longo de três anos que inclui licenciamento (150 mil a 180 mil euros por ano), integração e consultoria (50 mil a 150 mil euros no primeiro ano), formação (20 mil a 50 mil euros) e custos operacionais contínuos.

"O custo mais subestimado é o esforço humano: tempo das equipas internas para gerir mudanças, ajustar políticas e responder a incidentes", alerta o representante da Microsoft Portugal. "Muitos clientes focam-se no preço das licenças e ignoram que é necessário investir em pessoas e processos".

Ricardo Marciano indica que "a complexidade operacional quando se opta por múltiplos fornecedores" é sistematicamente subestimada. David Grave aponta que, "para 95% das empresas portuguesas, a plataforma única", em vez do *best-of-breed*, "vence. A complexidade de integrar cinco soluções cria lacunas de segurança onde os dados não fluem".

Para Manfred Ferreira, a abordagem deve ser contextual. "O ponto de partida passa por uma análise da realidade atual (*as-is*), da génese da organização e das suas necessidades imediatas e de médio prazo, permitindo definir prioridades claras e uma visão futura viável (*to-be*)". Em muitos cenários, a consolidação numa única plataforma *best-of-breed* apresenta vantagens claras. Noutros, mais específicos ou de nicho, uma abordagem *multi-vendor* pode revelar-se mais ade-

quada. "Cada situação deve ser analisada de forma individual, com foco nas necessidades reais da organização e no valor que pode ser gerado", defende.

ROADMAP E TIMELINE

David Grave recomenda uma sequência clara: identidade (consolidar diretórios, MFA forte), acesso condicional e ZTNA com visibilidade dos *endpoints*, segmentação de *workloads* críticos e microssegmentação com DLP. O *timeline* serão 12 a 18 meses para uma maturidade média.

Manfred Ferreira, da Noesis, propõe uma abordagem estrutura em três fases seguindo o conceito "*crawl, walk & run*":

• **Segurança da força de trabalho (*crawl*)**: três meses iniciais, podendo estender-se a 12 meses em grandes organizações. Foco *human-centric* com canais de acesso seguros baseados em ZTNA que substituem progressivamente as VPN tradicionais. Desde o primeiro dia, apenas utilizadores autenticados e autorizados, utilizando equipamentos conformes, acedem aos recursos adequados ao seu perfil. Esta transição deve abranger também prestadores de serviços externos – um vetor que, nos últimos anos, foi origem de parte significativa dos acessos indevidos;

• **Segurança dos data centers e cloud (*walk*)**: inicia-se tipicamente entre o terceiro e quarto mês, com duração de três a seis meses dependendo da complexidade das aplicações. Estende o zero trust às infraestruturas *on-premises*, ambientes híbridos, cloud (IaaS, PaaS, SaaS) e *workloads*. Permite inspeção transversal de ameaças, visibilidade dos fluxos de comunicação e controlo rigoroso dos acessos privilegiados com auditoria centralizada. Contribui para redução de latências e otimização de custos através da simplificação da arquitetura;

• **Segurança B2B e IoT/OT (*run*)**: representa a maturidade do modelo. Duração de quatro a oito meses, em função da heterogeneidade dos ambientes e nível de interação com parceiros. Aplica-se às comunicações B2B, ambientes críticos incluindo IoT/OT, sistemas *legacy* e acessos de terceiros. Inclui proteção de localizações remotas (sucursais, agências, quiosques) e novas tendências como motores de IA e LLM.

Um fator crítico, sublinha Manfred Ferreira, é a existência de conhecimento prévio da arquitetura e estrutura dos ambientes. Ricardo Marciano e Pedro Soares reforçam a importância de começar pequeno e evoluir progressivamente. "O zero trust não falha por ser restritivo; falha quando é aplicado sem contexto de negócio", defende Ricardo Marciano.

FUNCIONALIDADES COMPRADAS, MAS NÃO UTILIZADAS

Pedro Soares admite que os clientes adquirem pacotes completos, mas não usam funcionalidades avançadas. As ferramentas de microssegmentação granular são um exemplo frequente: "muitas empresas compram soluções sofisticadas, mas acabam por aplicar apenas regras básicas, porque mapear todas as

dependências entre aplicações é complexo e demorado". O resultado são funcionalidades *premium* que ficam paradas.

Módulos de análise avançada com IA em plataformas XDR ou SIEM seguem o mesmo padrão. "Os clientes adquirem Defender for Cloud Apps ou Sentinel esperando usar UEBA, mas não têm equipa para acompanhar alertas ou ajustar algoritmos e acabam por desligar porque geravam falsos positivos", explica o representante da Microsoft Portugal.

MANFRED FERREIRA, NOESIS

"É ESSENCIAL COMUNICAR À ORGANIZAÇÃO O PROPÓSITO DESTA JORNADA, OS OBJETIVOS E IMPACTOS ESPERADOS, PROMOVENDO PARTICIPAÇÃO ATIVA E MANTENDO A COMUNICAÇÃO ABERTA. SÓ ASSIM A TRANSIÇÃO SE TORNA RESPONSABILIDADE PARTILHADA"

MANFRED FERREIRA, BUSINESS DEVELOPER MANAGER DE CYBER SECURITY & NETWORK DA NOESIS

O mesmo acontece com o PAM sofisticado e proteção de dados com classificação automática, onde os "clientes compram soluções para etiquetar e encriptar informação sensível, mas não avançam com projetos de taxonomia, deixando a funcionalidade desligada".

Ricardo Marciano identifica "funcionalidades avançadas de automação e resposta contextual" compradas antes da maturidade operacional necessária. "O problema não é a tecnologia, é a falta de processos e confiança para delegar decisões à automação". A lição passar por fasear a adoção, garantindo que cada capacidade é utilizada de forma consistente antes de avançar para a seguinte.

O QUE OS CISO DEVEM FAZER

David Grave defende que o "zero trust é uma mudança de paradigma. E mudanças de paradigma falham mais por tentarmos concretizar de uma só vez projetos demasiado ambiciosos do que por causa da tecnologia. Não procurar a perfeição, procurar

a progressão". A recomendação para o representante da Claranet Portugal é começar por proteger o ativo mais crítico, como se o resto da rede já estivesse comprometida. "Muitos projetos morrem na fase de planeamento porque tentam mapear a organização inteira. A tecnologia é a parte fácil; mudar a cultura de confiança implícita para verificação explícita é o verdadeiro desafio".

Ricardo Marciano enquadra que "o zero trust é, acima de tudo, um exercício de gestão de risco e de clareza organizacional". Partindo do princípio de que nenhum utilizador ou dispositivo é automaticamente confiável, o essencial é medir tudo e aceitar que a infraestrutura deve ajustar-se constantemente. "Zero trust não deve ser visto como resultado, mas prática contínua. Quem entra à espera de chegar ao fim desiste rapidamente e quem entra para evoluir colhe resultados reais".

Pedro Soares estrutura em cinco pontos aquilo que, na sua opinião, os responsáveis de cibersegurança devem fazer: garantir patrocínio executivo visível do *board* e CIO; priorizar e fasear com *quick wins* (MFA universal, segmentação de acessos privilegiados) e *roadmap* com marcos trimestrais; investir em pessoas e processos, preparando equipas e comunicando mudanças aos utilizadores; medir e comunicar resultados com KPI claros desde o início; adotar melhoria contínua sem procurar perfecionismo. "A implementação não será linear: vão surgir exceções e ajustes. Mantenha os princípios e adapte regras quando necessário. Em zero trust, *done is better than perfect*".

Já Manfred Ferreira recomenda um *master plan* centrado em iniciativas alinhadas com as metas do negócio, permitindo identificar o valor de cada iniciativa, definir prioridades e estabelecer KPI suportados por observabilidade contínua. É fundamental integrar desde o início governação corporativa, cumprimento regulatório e aspetos operacionais relacionados com resiliência. "Mas não menos importante, a componente de cultura e pessoas. É essencial comunicar à organização o propósito desta jornada, os objetivos e impactos esperados, promovendo participação ativa e mantendo a comunicação aberta. Só assim a transição se torna responsabilidade partilhada".

Entre o mercado de 92 mil milhões de dólares projetados para 2030 e a realidade de que 75% das agências federais americanas vão falhar a implementação das suas políticas zero trust até 2026 segundo a Gartner, fica clara a distância entre aspiração e execução.

O consenso entre os quatro especialistas é unânime: zero trust não é um produto que se compra, é uma jornada que exige estratégia, governança e mudança cultural. As organizações que tratam a implementação como um projeto tecnológico isolado em vez de uma transformação organizacional sustentada estão, quase inevitavelmente, destinadas a juntar-se às estatísticas de falhar.◀

claranet®

por David Grave,
Security Director, Claranet Portugal

CIBERSEGURANÇA NA ERA DOS DEEPFAKES: PROTEGER A CONFIANÇA

DURANTE DÉCADAS, A CIBERSEGURANÇA CONSTRUIU-SE SOBRE UMA PREMISSA CONFORTÁVEL: PROTEGER SISTEMAS, REDES E DADOS. FALÁVAMOS DE PERÍMETRO E DAS JOIAS DA COROA: FIREWALLS, EDR, SIEM, ZERO TRUST, PENTESTING... TUDO GIRAVA EM TORNO DA INFRAESTRUTURA. ENQUANTO NOS TORNÁMOS EXCELENTES A PROTEGER MÁQUINAS, NEGLIGENCIÁMOS AQUILO QUE REALMENTE MOVE O NEGÓCIO: A CONFIANÇA. HOJE, OS ATACANTES JÁ NÃO PRECISAM DE EXPLORAR UMA VULNERABILIDADE NUM SERVIDOR: BASTA EXPLORAREM UMA VULNERABILIDADE NA NOSSA PERCEÇÃO DA REALIDADE.

Durante anos repetimos o mantra: "o ser humano é o elo mais fraco". Investimos milhões em formação, awareness e simulações de phishing convencidos de que, se treinássemos as pessoas para "olhar com atenção", estaríamos mais seguros. Essa era acabou.

A VERDADE TORNOU-SE MALEÁVEL

Num mundo em que alguns segundos de áudio permitem clonar a voz de um CFO e um modelo open-source consegue criar um rosto quase autêntico, em tempo real, a atenção humana tornou-se um risco operacional.

Se a nossa estratégia de *segurança* depende de um colaborador conseguir distinguir, numa videochamada, se o CEO é real ou um avatar gerado por IA, então a nossa estratégia já falhou. Se a identidade é o novo perímetro, os deepfakes são o novo cavalo de Tróia?

Continuar a tratar os deepfakes como um tema emergente, interessante, mas não prioritário, pode

DAVID GRAVE, SECURITY DIRECTOR, CLARANET PORTUGAL

ser um erro. Não porque isto seja o apocalipse digital que os media adoram vender, mas porque os atacantes já ultrapassaram a fronteira da infraestrutura e entraram no território da confiança organizacional.

Já sabemos que não é "se" a organização será alvo de fraude - a pergunta é quando, e se vamos perceber a tempo.

Vamos desmistificar: isto não é apenas sobre vídeos hiper-realistas do CEO a pedir transferências bancárias - embora isso já esteja a acontecer, com taxas de sucesso preocupantes. O que existe hoje é um ecossistema criminoso em plena transformação, com adoção acelerada deste tipo de ferramentas, em ataques como:

- Identity Fraud: bancos, seguradoras e fintechs enfrentam tentativas diárias de abertura de contas com documentos "perfeitos", gerados por IA. Dados reais (NIF, número de telefone, IBAN), combinados com identidades fictícias, que passam validações e tornam-se ideais para fraude financeira, crédito, etc.
- Voice Cloning em Engenharia Social: alguns segundos de áudio retirados de um vídeo institucional no YouTube. Resultado: uma chamada "urgente" ao departamento financeiro, com a voz exata do CEO ou CFO.

ONDE A DETEÇÃO FALHA (E PORQUE ISSO IMPORTA)

A tecnologia de *deteção* de deepfakes está, neste momento, dois passos atrás da tecnologia de criação. As abordagens atuais tentam detetar indicadores biométricos, com análises ao áudio e ao vídeo, através de micro-anomalias, iluminação ou inconsistências de pixéis.

Contudo, os modelos de Machine Learning que aplicamos para *deteção* são também usados na melhoria nos modelos.

A *defesa contra deepfakes* e fraudes de identidade exige uma abordagem radicalmente diferente: Trust, But Always Verify. Sem Exceções.

Implementem uma cultura de *segurança* saudável, onde validação de identidade é protocolo. Qualquer pedido sensível deve ser confirmado através de um canal alternativo pré-estabelecido, com um processo forte de verificação de decisões e confirmação multi-canal para decisões de alto impacto.

CONFIAR, MAS VERIFICAR – SEM EXCEÇÕES

Invistam em "Human Firewall" – desta vez, a sério. Não, não é mais um slide de PowerPoint sobre phishing. É treino prático, realista e contínuo. Simulações de ataques, exercícios de validação de identidade sob pressão e de Red Team, que testem não só tecnologia, como processos e pessoas.

Os deepfakes não são invencíveis. São apenas o próximo capítulo na eterna corrida entre ataque e defesa – a diferença é que, desta vez, a adaptação não é só tecnológica. É cultural. É estratégica. É de liderança.

As organizações que se vão defender melhor e adaptar a esta alteração de paradigma acelerado não serão as que adotaram a melhor ferramenta de *deteção*, mas sim as que tiverem processos onde verificar é reflexo e confiança é desenhada, não assumida. ◀

por Ricardo Carvalho,
Senior Security Consultant - CSO

ZERO TRUST:

FROM BUZZWORD TO REAL IMPLEMENTATION

"NUNCA CONFIAR, VERIFICAR SEMPRE" É FÁCIL DIZER REPETIDAMENTE, NO ENTANTO DIFÍCIL DE EXECUTAR.

O modelo Zero Trust, conforme formalizado pelo NIST na Publicação Especial 800-207, afasta-se da noção de uma rede interna implicitamente confiável. Em vez disso, cada pedido de acesso é avaliado de forma dinâmica, com base na identidade, no estado do dispositivo, nas políticas e na telemetria em tempo real. O objetivo não é reforçar o perímetro, mas tomar decisões mais precisas e contínuas, excluindo por completo o conceito tradicional de perímetro como elemento central da segurança.

Na prática, Zero Trust representa uma mudança profunda de mentalidade, obrigando as organizações a repensar a forma como o acesso é concedido, monitorizado e revogado ao longo do tempo.


RICARDO CARVALHO, SENIOR SECURITY CONSULTANT, CSO

NA PRÁTICA QUE SIGNIFICA ZERO TRUST:

- **Definir primeiro a superfície a proteger**

Implementações bem-sucedidas começam por identificar aplicações críticas, dados sensíveis e serviços essenciais. As políticas de acesso são então construídas em função de quem pode aceder

a esses recursos e em que condições. As orientações oficiais são consistentes ao defender uma adoção incremental, em vez de transformações disruptivas de uma só vez, reduzindo riscos operacionais e facilitando a mudança organizacional.

• **Passar do acesso à rede para o acesso à aplicação**

Conceder conectividade ampla à rede cria exposição desnecessária. Os modelos modernos de Zero Trust substituem esta abordagem por acesso por aplicação e por sessão. A conectividade só é estabelecida após a validação da identidade e do contexto, reduzindo a superfície de ataque e limitando o movimento lateral, mesmo em cenários de comprometimento.

• **Tratar identidade e postura do dispositivo como centrais**

As credenciais do utilizador, por si só, já não são suficientes. Arquiteturas Zero Trust maduras avaliam continuamente o estado do dispositivo, a integridade do sistema operativo e a postura de segurança em conjunto com a identidade. As decisões de acesso adaptam-se automaticamente à medida que o nível de risco muda.

• **Aplicar o princípio do menor privilégio de forma contínua**

A confiança implícita é eliminada. Os privilégios são estritamente limitados, temporários e revalidados ao longo da sessão. Esta abordagem reduz significativamente o impacto de credenciais comprometidas e de ameaças internas, melhorando a capacidade de contenção.

• **Aplicar políticas de forma consistente em todos os ambientes**

À medida que as aplicações se distribuem entre datacenters, plataformas cloud e serviços SaaS, a aplicação das políticas deve acompanhar utilizadores e aplicações. Os modelos de segurança entregues a partir da cloud fornecem, cada vez mais, uma camada unificada de políticas, garantindo controlos consistentes independentemente da localização.

DA TEORIA À IMPLEMENTAÇÃO

Um possível percurso pragmático segue normalmente três fases:

• **Fase 1**: Identificar aplicações de elevado valor, integrar fontes de identidade e iniciar pilotos de acesso ao nível da aplicação.

• **Fase 2**: Expandir a cobertura, incorporar verificações da postura dos dispositivos e reduzir a dependência de modelos tradicionais de acesso remoto.

• **Fase 3**: Utilizar telemetria para refinar políticas, minimizar privilégios permanentes e restringir ainda mais o movimento lateral.

O Zero Trust não é um produto isolado. É um modelo operacional assente na verificação contínua, no menor privilégio e no controlo de acesso preciso. Quando implementado de forma metódica, deixa de ser uma buzzword e passa a representar uma melhoria mensurável, sustentável e alinhada com os desafios atuais da postura de segurança. ◀

por Gianpietro Cutolo,
Cloud Security Researcher, Netskope

COMO CONSTRUIR UM MODELO ZERO TRUST NUM MUNDO DE LLM

COM A CRESCENTE PRESENÇA DOS LARGE LANGUAGE MODELS (LLM) EM DIVERSOS AMBIENTES DE TRABALHO, O MODEL CONTEXT PROTOCOL (MCP) TEM-SE CONSOLIDADO COMO UM ELEMENTO FUNDAMENTAL DOS ASSISTENTES DE INTELIGÊNCIA ARTIFICIAL.

O MCP funciona como uma interface universal que permite aos LLM ligarem-se facilmente a sistemas externos sem compreenderem o seu conteúdo. Em software e engineering, acelera a automação de tarefas e facilita workflows diários como o onboarding de utilizadores, o resumo de emails ou o agendamento de eventos.

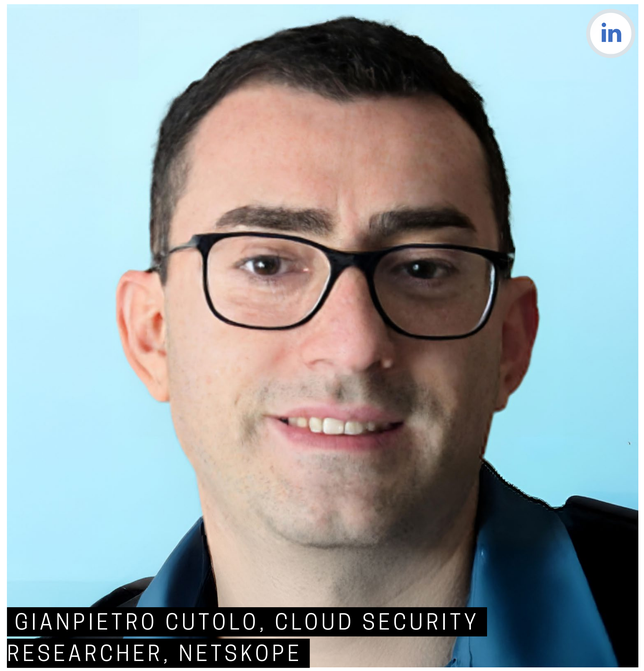
Embora o MCP ofereça vantagens ao nível da integração, também aumenta a superfície de ataque ao delegar confiança em produtos, logs e servers. Isto permite que os cibercriminosos explorem a sua flexibilidade e credulidade, levando os produtos MCP a aceitarem informação sem verificar a sua legitimidade.

Neste processo, os adversários já não precisam de comprometer o próprio modelo. Em vez disso, exploram as camadas de construção de contexto acumuladas pelo MCP: metadata, descrições e o response flow das ferramentas que os LLM assumem como “verdades” fidedignas.

EXPLOITS QUE ESTÃO A GANHAR RELEVÂNCIA

Tendo em conta estas estratégias, observamos a consolidação de certos tipos de ataques que os frameworks de segurança tradicionais não conseguem mitigar de forma direta.

- **Injeção de startup prompt através de definições de ferramentas**: Os MCP servers fornecem aos LLMs


GIANPIETRO CUTOLO, CLOUD SECURITY RESEARCHER, NETSKOPE

ferramentas com descrições inseridas no startup prompt, permitindo que atacantes manipulem os modelos ao registar tools que exfiltram ou alteram sensitive data.

• **Sombreamento de ferramentas entre servidores**: Quando vários servidores MCP partilham contexto e não estão devidamente isolados, uma ferramenta maliciosa pode propagar instruções escondidas e comprometer todo o ambiente.

• **Troca maliciosa de ferramentas (*rug pull*)**: Os adversários podem modificar registries ou mecanismos de atualização para substituir ferramentas legítimas por versões maliciosas, conseguindo roubar chaves API ou executar ações prejudiciais sem gerar alertas.

• **Injeção de códigos ANSI**: Os atacantes utilizam códigos ANSI para ocultar instruções maliciosas nas descrições de ferramentas do MCP, tornando-as invisíveis para o utilizador, mas interpretáveis pelos modelos de IA.

PASSOS PRÁTICOS PARA UMA DEFESA ZERO TRUST

Uma defesa eficaz deve aplicar princípios de Zero Trust às ferramentas, verificação criptográfica, monitorização de comportamento e isolamento rigoroso dos servidores MCP. Eis cinco formas de o fazer:

• **Procedência do registo**: apresenta apenas ferramentas provenientes de registos verificados que exijam assinatura digital, garantindo a autenticidade e evitando manipulações.

• **Barreiras de proteção**: aplica filtros e classificadores automáticos para detetar e remover possíveis prompt injections nos fluxos de entrada e saída.

• **Isolamento em camadas**: separa os metadados das ferramentas por servidor, carregando apenas os necessários e renovando o contexto para excluir descrições irrelevantes, especialmente em ferramentas sensíveis. Utiliza servidores distintos para áreas que exijam proteção adicional.

• **Restrição de permissões**: limita as ferramentas aos privilégios mínimos necessários, de acordo com uma abordagem Zero Trust, regista e revê periodicamente as permissões e remove as que já não são necessárias.

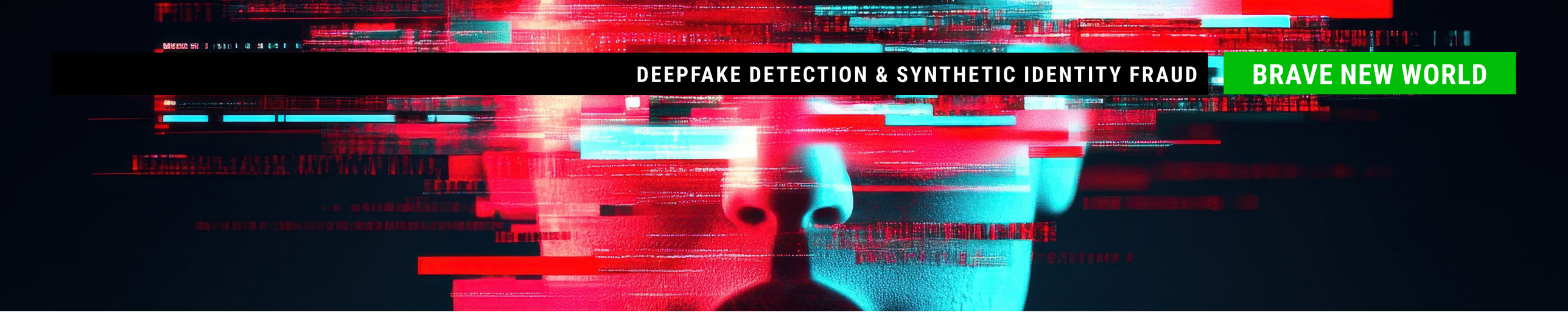
• **Avaliação de risco**: atribui uma classificação de risco a cada servidor MCP para priorizar a atenção sobre aqueles com maior potencial de impacto.

O primeiro passo para assegurar integrações MCP seguras passa por compreender o papel dos assistentes de IA no ecossistema digital. Um MCP executa todas as instruções que são injetadas no seu contexto. A adoção de uma estratégia de defesa **multicamada baseada em Zero Trust** — que inclua auditoria de origem, barreiras de proteção, isolamento, permissões mínimas e análise de risco — permite que a integração de LLM gere valor para a organização, em vez de introduzir novos vetores de risco. ◀

POR RUI DAMIÃO

DEEPFAKES: A NOVA FRONTEIRA DA FRAUDE EMPRESARIAL

AS TENTATIVAS DE FRAUDE COM DEEPFAKES AUMENTARAM 2.137% EM TRÊS ANOS E CUSTARAM ÀS EMPRESAS UMA MÉDIA DE 500 MIL DÓLARES POR INCIDENTE. O PROBLEMA VAI PARA ALÉM DAS TECNOLOGIAS DE DETEÇÃO E ENTRA NOS PROCESSOS QUE NÃO ACOMPANHAM A EVOLUÇÃO DAS AMEAÇAS.



O crescimento de tentativas de fraude baseadas em deepfakes está a transformar a forma como as organizações gerem risco e validam identidades. Segundo o relatório "*The Battle Against AI-Driven Identity Fraud*" da Signicat, as tentativas aumentaram 2.137% entre 2022 e 2025. A Deepstrike, por sua vez, aponta que o volume passou de 500 mil ocorrências em 2023 para uma projeção de oito milhões de tentativas em 2025.

O impacto financeiro é elevado; segundo a Entrust, deepfakes ocorrem agora a cada cinco minutos e as empresas perderam, em média, 500 mil dólares por incidente em 2024. As projeções indicam que as perdas por fraude facilitada por Inteligência Artificial (IA) generativa nos Estados Unidos vão atingir os 40 mil milhões de dólares até 2027.

Luís Catarino, Head of Offensive Security Iberia na Thales, afirma que, "nas investigações forenses, os casos mais frequentes são deepfakes usados como peça de esquemas de fraude mais amplos. Em particular, vemos deepfakes em fraude de pagamento de faturas e em chantagem dirigida a executivos de topo".

A REDEFINIÇÃO DO RISCO

O caso da empresa Arup tornou-se numa referência global e é sobejamente conhecido na área. Em fevereiro de 2024, um colaborador da empresa participou numa videoconferência onde via o que acreditava ser o CFO e outros executivos. Recebeu instruções para várias transferências, totalizando 25 milhões de dólares. Todas as pessoas, no entanto, eram avatares gerados por IA. Bruno Castro, Fundador & CEO da VisionWare, reconhece que este tipo de ataques "demonstra a eficácia da combinação entre engenharia social, manipulação visual em tempo quase real e exploração da confiança".

Luís Catarino menciona uma tentativa de ataque em julho de 2024, onde um executivo da Ferrari conseguiu travar um ataque quando percebeu que a voz do suposto CEO, embora extremamente convincente, "não respondeu corretamente a uma pergunta pessoal". Os atacantes replicaram não só a voz de Benedetto Vigna, mas também o seu sotaque regional e maneirismos numa tentativa de legitimar um pedido de "aquisição urgente".

Estes exemplos mostram como a realidade está a mudar. Um estudo da Pindrop documenta um aumento de 1.300% nas tentativas de fraudes a envolver deepfakes durante o ano de 2024 e, de acordo com a Keepnet, os esquemas de phishing com deepfake "estão a tornar-se cada vez mais difíceis de detetar", com as perdas na América do Norte a terem ultrapassado os 200 milhões de dólares no primeiro trimestre de 2025. "Torna-se importante para as pessoas e para as organizações perceber o risco", diz o relatório da Keepnet.

O IMPACTO DOS FALSOS POSITIVOS

Sistemas demasiado agressivos geram falsos positivos que bloqueiam operações legítimas. Luís Catarino explica que "estudos de fornecedores como SEON e Sift apontam para taxas históricas de falsos positivos na ordem dos 8 a 10% em sistemas baseados em regras, o que significa, em organizações de grande volume, milhares de transações legítimas bloqueadas ou marcadas para revisão todos os dias". A taxa aceitável situa-se abaixo de 3%.

Bruno Castro reforça que "a taxa aceitável depende sempre do risco do processo e do valor protegido, mas o objetivo deve ser manter um equilíbrio rigoroso entre segurança, fluidez operacional e capacidade de resposta humana".

O que se constrói, na prática, é uma arquitetura em camadas com "modelos de IA a reduzir o universo de casos suspeitos, regras de negócio a definir onde se aceita mais fricção, e validação humana nos pontos onde uma decisão errada é inaceitável", descreve Luís Catarino, da Thales.


BRUNO CASTRO, VISIONWARE

SOFISTICAÇÃO ONDE NÃO SE ESPERA

Um caso anonimizado descrito por Luís Catarino ilustra a natureza dos ataques. Numa multinacional, o atacante comprometeu o email de um fornecedor real, observou durante semanas o padrão de comu-

"A TAXA ACEITÁVEL DEPENDE SEMPRE DO RISCO DO PROCESSO E DO VALOR PROTEGIDO, MAS O OBJETIVO DEVE SER MANTER UM EQUILÍBRIO RIGOROSO ENTRE SEGURANÇA, FLUIDEZ OPERACIONAL E CAPACIDADE DE RESPOSTA HUMANA"

nicação e pediu alteração do IBAN anexando o documento de autorização com assinatura do CFO. "Neste caso, o elemento IA não era um vídeo impressionante, mas uma assinatura num ficheiro PDF", explica. "O logótipo, o formato, a linguagem e a assinatura correspondiam ao que a equipa esperava ver, o domínio de email era legítimo e o valor da fatura encaixava no histórico. O pagamento foi feito sem qualquer suspeita", conta.

O processo falhou em múltiplos pontos. Não havia validação por segundo canal para mudanças de dados bancários. A equipa não questionou uma alteração de IBAN que chegou por email, mesmo tratando-se de um fornecedor com anos de relacionamento estável. Não existia reconciliação frequente que permitisse detetar rapidamente que o dinheiro não tinha chegado. A assinatura no PDF era uma imagem sintetizada a partir de amostras anteriores, disponíveis em dezenas de documentos legítimos. "Muitas vezes, é uma pequena peça sintética inserida num processo que, de resto, parece perfeitamente normal", alerta o representante da Thales.

LIMITES NA DETEÇÃO

A tecnologia de deteção enfrenta limitações significativas. Segundo a Brightside, modelos treinados em laboratório chegam a 95% de precisão, mas com videochamadas comprimidas e iluminação medíocre, os resultados podem cair 45 a 50 pontos percentuais, partilha Luís Catarino.

O problema não é apenas tecnológico, mas também humano. Estudos apontam que a taxa de deteção humana de deepfakes de alta qualidade em vídeo é bastante baixa, indicando que três em cada quatro pessoas não conseguem identificar um vídeo falso sofisticado. Esta incapacidade humana torna crítica a necessidade de processos que não dependam da capacidade de julgamento individual.

Bruno Castro, da VisionWare, reconhece que "a tecnologia atual é mais eficaz na identificação de conteúdos de menor sofisticação, frequentemente designados por *cheapfakes*". Já Luís Catarino alerta para ataques de injeção de vídeo, em que os atacantes "recorrem a câmaras virtuais e software de *face-swap* para injetar vídeo sintético no fluxo".

Bruno Castro acrescenta que existem "limitações relevantes nas abordagens baseadas em *watermarking*" uma vez que estas marcas "não são universais, podem ser removidas ou degradadas por compressão, recodificação ou simples edição, e dependem fortemente da adoção voluntária por parte de plataformas e fornecedores, o que reduz a sua eficácia como mecanismo de confiança transversal".

A criação de deepfakes evolui mais rapidamente do que a deteção. Bruno Castro refere que existem "modelos generativos cada vez mais acessíveis, baratos e fáceis de utilizar que acelera a capacidade do cibercrime" enquanto, do lado da deteção, "cada nova técnica de ataque exige recolha de dados, etiquetagem, treino, validação e integração, num ciclo que se mede em semanas ou meses", explica Luís Catarino.


LUÍS CATARINO, THALES

AMEAÇAS EMERGENTES

Luís Catarino identifica três evoluções nas ameaças com deepfakes. A primeira é a síntese em tempo real que torna difícil distinguir o "pré-gravado" de "ao vivo". Em segundo lugar são as redes de identidades sintéticas que se comportam de forma credível durante meses antes de entrarem em ação coordenada.

O terceiro é a infiltração de equipas remotas; os casos de trabalhadores IT norte-coreanos mostram isso mesmo. De acordo com o Office of Financial Sanctions Implementation e a Palo Alto Networks, milhares de trabalhadores norte-coreanos conseguiram empregos remotos em empresas ocidentais usando identidades roubadas, perfis fabricados no

> "ASSUMIR QUE NEM AS PESSOAS NEM OS SISTEMAS DA ORGANIZAÇÃO CONSEGUEM, POR DEFEITO, DISTINGUIR COM FIABILIDADE UM EXECUTIVO REAL DE UM CLONE DE IA"

LinkedIn com fotos geradas por inteligência artificial e proxies humanos nas entrevistas. Uma vez contratados, operam através de VPN que escondem a sua localização, canalizando salários para Pyongyang e obtendo acesso a código-fonte e infraestruturas críticas. Para empresas que contratam remotamente, este risco pode, até, ter implicações legais graves.

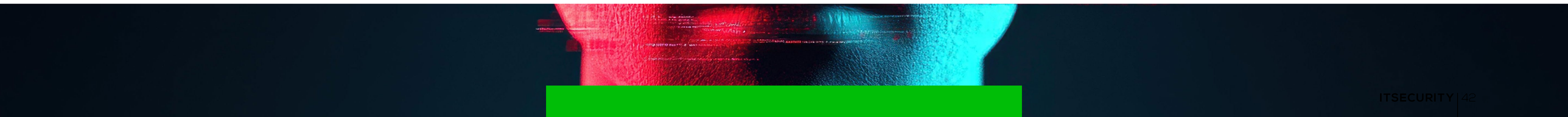
MEDIDAS IMEDIATAS (SEM ORÇAMENTO)

Questionados sobre o que faziam imediatamente mesmo sem orçamento específico para tecnologia de deteção de deepfakes, Luís Catarino defende que a primeira decisão seria concetual e não tecnológica. “Assumir que nem as pessoas nem os sistemas da organização conseguem, por defeito, distinguir com fiabilidade um executivo real de um clone de IA”. As medidas imediatas são, assim, regras simples, como nenhuma transferência acima de determinado montante pode ser aprovada apenas por email ou chamada; mudanças de IBAN devem ser validadas por um canal secundário; decisões “urgentes” fora de horas exigem segunda confirmação.

No caso da alteração de dados bancários de fornecedor, por exemplo, deve ser feito um contacto utilizando sempre o número que consta no contrato original e nunca o que vem no email. Para transferências acima do valor estipulado, exigir a aprovação de duas pessoas de departamentos diferentes, sendo que pelo menos uma após contacto telefónico direto. Para pedidos urgentes fora do horário normal, pode-se implementar uma espera de 24 horas ou validação presencial.

Bruno Castro propõe três pilares: “prevenção antes do incidente com auditorias e formação; deteção durante o incidente com monitorização e alarmística; reação após o incidente com definição clara de resposta e recuperação”.

Investir não significa apenas comprar tecnologia, mas alocar tempo sobre processos críticos, formação de equipas e avaliação de soluções. Como sintetiza Luís Catarino, “as organizações que fizerem este trabalho de base agora estarão melhor posicionadas não apenas para evitar o próximo incidente, mas também para demonstrar que levam a sério um problema que deixou de ser ficção científica para se tornar rotina de investigação forense”.◀



OLIVIA ARANTES É ENGENHEIRA INFORMÁTICA, COM PÓS-GRADUAÇÃO EM CIBERSEGURANÇA E MESTRADO EM SEGURANÇA DA INFORMAÇÃO E DIREITO NO CIBERESPAÇO. CISO E DIRETORA DE SEGURANÇA DA IMPRENSA NACIONAL-CASA DA MOEDA, LIDERA A ESTRATÉGIA DE PROTEÇÃO DA INFORMAÇÃO E GESTÃO DO RISCO CIBERNÉTICO.

POR OLIVIA ARANTES, INCM

A AMEAÇA INTERNA: UM RISCO SUBESTIMADO NAS ORGANIZAÇÕES

UMA PARTE SIGNIFICATIVA DO ESFORÇO DIÁRIO DAS EQUIPAS DE CIBERSEGURANÇA É DEDICADA À MITIGAÇÃO DE VULNERABILIDADES TÉCNICAS, MUITAS VEZES GUIADA POR LISTAS EXTENSAS E EM CONSTANTE CRESCIMENTO

Nem sempre, porém, esta abordagem é verdadeiramente baseada no risco, permitindo identificar quais as vulnerabilidades cuja exploração teria maior impacto real na exposição da organização.

Vivemos numa corrida constante para resolver todos os riscos que surgem, quase de forma automática, enquanto ameaças mais relevantes podem estar a passar despercebidas. Foi precisamente por isso que decidi escrever este artigo sobre a ameaça interna (insider threat), um risco frequentemente subestimado.

A ameaça interna é aquela que bebe café connosco, que se senta ao nosso lado nas reuniões e que tem acesso às nossas instalações e aos nossos sistemas. Costuma

> "A AMEAÇA INTERNA É AQUELA QUE BEBE CAFÉ CONNOSCO, QUE SE SENTA AO NOSSO LADO NAS REUNIÕES E QUE TEM ACESSO ÀS NOSSAS INSTALAÇÕES E AOS NOSSOS SISTEMAS. COSTUMA DIZER SE QUE INFORMAÇÃO É PODER, E NESTE CONTEXTO ISSO É INEGAVELMENTE VERDADE"

dizer se que informação é poder, e neste contexto isso é inegavelmente verdade. Esta ameaça caracteriza se pelo envolvimento de colaboradores, prestadores de serviços ou parceiros que possuem acessos legítimos aos sistemas, infraestruturas e informação da organização. O principal desafio reside no facto de estes atores operarem, inicialmente, dentro dos limites da autorização que lhes foi concedida, explorando relações de confiança pré existentes.

Fatores como desmotivação, conflitos internos, desalinhamento com a estratégia da organização, frustração profissional ou coerção externa podem conduzir a comportamentos de risco. Importa salientar que este cenário não se limita a utilizadores com acessos privilegiados. Colaboradores com níveis de acesso aparentemente reduzidos podem, ainda assim, ter acesso a informação sensível ou crítica para o negócio.

A pergunta que se impõe é simples: a sua organização tem visibilidade suficiente sobre o comportamento dos seus próprios utilizadores?

Durante muito tempo, sempre que este tema era abordado, a resposta surgia quase automaticamente: “os nossos colaboradores têm acordos de confidencialidade”. É verdade, mas estes mecanismos, por si só, são insuficientes. Quando uma organização sofre um dano reputacional, todos perdem. E esse dano pode levar anos a ser recuperado ou, em alguns casos, nunca o ser totalmente.

Deixo outra questão para reflexão: quando foi a última vez que identificou um colaborador claramente descontente com a organização?

Precisamos de abordar este risco de forma racional. Os colaboradores circulam diariamente pela organização e muitos possuem acessos privilegiados que, por vezes, podem ser utilizados sem uma justificação evidente. Mesmo quando são solicitadas justificações, estas tendem a ser plausíveis: interven-

ções fora de horas, reinício de serviços críticos ou resolução urgente de incidentes.

Sabemos que vamos ter de viver com este risco, mas isso não implica viver num estado permanente de desconfiança. Não é esse o objetivo. O caminho passa pela implementação de processos sólidos, baseados no conceito de Zero Trust.

De forma simples, o Zero Trust assenta no princípio da confiança zero, ou seja, ninguém interno ou externo deve ser automaticamente considerado confiável. No contexto de acessos privilegiados, isto traduz se na exigência de mais do que uma validação para executar ações sensíveis, garantindo que nenhum utilizador atua de forma isolada e sem controlo.

Na prática, isto significa recorrer a mecanismos como autenticação forte, dupla validação, segregação de funções e controlo de acessos baseado no contexto. Tecnologias como Identity and Access Management (IAM) e Privileged Access Management (PAM) permitem gerir quem acede a quê, quando e em que condições, reduzindo significativamente o risco de abuso de privilégios.

"ACREDITO QUE O FUTURO DA CIBERSEGURANÇA ORGANIZACIONAL PASSARÁ INEVITAVELMENTE POR MODELOS QUE PRIVILEGIEM MENOS CONFIANÇA IMPLÍCITA E MAIOR VERIFICAÇÃO CONTÍNUA, COM PROCESSOS DESENHADOS PARA FUNCIONAR NA PRÁTICA E NÃO APENAS PARA CUMPRIR REQUISITOS FORMAIS"

A monitorização ativa e contínua dos acessos é igualmente crítica, sobretudo fora do horário normal de operação e ao fim de semana. A análise de padrões de comportamento e a deteção de desvios como acessos não habituais, volumes anormais de dados ou alterações no perfil de utilização permitem identificar potenciais situações de comprometimento numa fase inicial.

Acredito que o futuro da cibersegurança organizacional passará inevitavelmente por modelos que privilegiem menos confiança implícita e maior verificação contínua, com processos desenhados para funcionar na prática e não apenas para cumprir requisitos formais.

Fica a nota final: alterações de comportamento nos utilizadores devem ser tratadas como indicadores relevantes de risco e integradas de forma consistente na estratégia de segurança.

TERESA PEREIRA, TAMBÉM CONHECIDA COMO STARMTP, TRABALHA ATUALMENTE COMO CYBER THREAT HUNTER. JÁ PARTILHOU O SEU CONHECIMENTO EM DIVERSAS CONFERÊNCIAS NACIONAIS E INTERNACIONAIS, E TEM EXPERTISE EM THREAT HUNTING, SEGURANÇA DE APIS, OSINT E ENGENHARIA SOCIAL. EM 2025 PARTICIPOU NA COMPETIÇÃO DE VISHING DA DEFCON 33, EM LAS VEGAS, ONDE ALCANÇOU O 8º LUGAR.

POR TERESA PEREIRA

BRAIN HACK: QUANDO A CONFIANÇA SE TORNA UMA VULNERABILIDADE

"NA CONFIANÇA ESTÁ O PERIGO" - UM PROVÉRBIO TÃO POPULAR, APLICÁVEL A DIVERSAS ÁREAS DA NOSSA VIDA. COM O PASSAR DOS ANOS E OS AVANÇOS TECNOLÓGICOS, A CIBERSEGURANÇA TORNOU-SE UMA PARTE INTEGRANTE DO NOSSO QUOTIDIANO, E ESTE PROVÉRBIO VOLTOU A GANHAR RELEVÂNCIA

A Cibersegurança já não se limita a proteger apenas sistemas e dados. Atualmente, o fator humano é também uma vulnerabilidade, sendo cada vez mais o alvo preferido dos atacantes, necessitando de proteção não apenas por parte dos especialistas da área, mas por todos nós, enquanto sociedade.

De acordo com o *relatório* de Resposta a Incidentes da Palo Alto lançado em Fevereiro de 2025, os atacantes exploram várias frentes para aceder a dados ou sistemas sensíveis de uma empresa. No Top 3, em 2º lugar, encontra-se a frente humana, com 65% de casos registados, segundo as estatísticas. A exploração do fator huma-

no, influenciando alguém a realizar uma ação ou a revelar dados, mesmo que não seja algo do seu interesse, é conhecida como Engenharia Social. No século XXI, é raro o cidadão que nunca recebeu um email, uma mensagem de texto ou uma chamada fraudulenta - Phishing, Smishing e Vishing, respetivamente. É importante notar que aqui falamos de Engenharia Social aplicada à Cibersegurança, embora esta possa ser aplicada a outras áreas, como Vendas e Marketing.

A Engenharia Social explora várias características humanas além da confiança, como a vergonha, o medo e a curiosidade. No final do dia, não são exploradas vulnerabilidades técnicas, mas sim vulnerabilidades psicológicas, com consequências potencialmente catastróficas para as empresas, incluindo perda de dinheiro e reputação. Os atacantes têm diversas motivações, como dinheiro, fama e reconhecimento. Se houver um atalho, uma vulnerabilidade que exige menos tempo para explorar e oferece o mesmo tipo de acesso, eles irão escolhê-la.

"A ENGENHARIA SOCIAL EXPLORA VÁRIAS CARACTERÍSTICAS HUMANAS ALÉM DA CONFIANÇA, COMO A VERGONHA, O MEDO E A CURIOSIDADE. NO FINAL DO DIA, NÃO SÃO EXPLORADAS VULNERABILIDADES TÉCNICAS, MAS SIM VULNERABILIDADES PSICOLÓGICAS, COM CONSEQUÊNCIAS POTENCIALMENTE CATASTRÓFICAS PARA AS EMPRESAS, INCLUINDO PERDA DE DINHEIRO E REPUTAÇÃO"

Porquê gastar horas ou dias a explorar uma vulnerabilidade técnica quando se pode obter o mesmo tipo de acesso após alguns minutos numa chamada de Vishing?

Além das campanhas em massa (e.g. Mass-Phishing), as campanhas mais focadas num alvo (e.g. Spear-Phishing), seja uma organização ou um indivíduo, envolvem uma investigação prévia. Esta investigação, conhecida como OSINT (Open-Source Intelligence), envolve não só Dorking - utilização de queries avançadas em browsers (e.g. Google) para localizar informação que pode não ser facilmente acessível através da pesquisa convencional - mas também redes sociais e outras ferramentas criadas para o efeito. Quanto mais exaustiva for a investigação, mais bem construída e credível será a campanha.

Em termos de campanhas, as mais bem-sucedidas para os atacantes envolvem temas como benefícios, prémios, encomendas, investimentos, bónus e salário. Já os nossos antepassados diziam: "Quando a esmola é grande, o pobre desconfia".

Para aumentar a credibilidade e sucesso dos ataques de Engenharia Social, nos últimos anos foi adicionado um novo ingrediente à equação: a

Inteligência Artificial. O uso de Deepfakes, seja por imagem ou áudio, permite utilizar vozes e imagens familiares ao alvo.

Existem já várias ferramentas no mercado que permitem que qualquer cidadão comum (não apenas pessoas com conhecimento técnico) consiga clonar a voz de outra pessoa ou falsificar uma imagem ou vídeo, pagando apenas uma quantia simbólica. O denominado "AI Slop" inunda as nossas redes sociais diariamente, tornando cada vez mais complexo para o ser humano identificar se o que está a ouvir ou ver é real ou gerado por Inteligência Artificial.

Algumas das campanhas de Engenharia Social que recorrem ao uso de Inteligência Artificial, em Portugal, ainda nos permitem distinguir que não são reais, mas sim fabricadas. Contudo, num futuro próximo, será quase impossível distinguir o que é real do que é falso. E nessa altura, o que fazemos? Devemos confiar? Ou devemos, primeiramente, duvidar e confirmar?

Apenas ao questionarmos conseguimos verificar se uma chamada, email ou mensagem de texto provém de uma fonte legítima. No caso dos emails, existem várias maneiras de confirmar a sua autenticidade, como analisar os cabeçalhos, o corpo do email - incluindo a forma como é escrito (verificando erros ortográficos ou outras pistas que indiquem que poderá ser Phishing, como urgência, links suspeitos ou maliciosos e intimidação para realizar uma ação dentro de um prazo estipulado), a assinatura do email e o remetente. Contudo, atualmente é comum o uso de técnicas de Spoofing, onde, devido a configurações incorretas nos registos de autenticação de email (SPF, DKIM e DMARC), é possível usar um domínio legítimo como máscara para enviar emails que parecem autênticos. Em casos de mensagens de texto, deveremos verificar o ID do remetente (caso não haja spoofing), a presença de links suspeitos ou maliciosos e a forma como a mensagem é escrita, de maneira semelhante à análise de emails referida anteriormente.

Finalmente, no caso de chamadas telefónicas, é importante confiar no nosso sexto sentido e também prestar atenção ao que nos é solicitado. Se o pedido for incomum ou parecer estranho, devemos desligar e ligar para o número oficial da empresa que supostamente nos contactou. Se houver suspeita de Spoofing, onde um número real (caller ID) é utilizado como máscara, é aconselhável desligar e ligar novamente para confirmar a origem da chamada. É crucial lembrar que o Spoofing é apenas uma máscara, não garantindo que o contacto foi realmente feito a partir de uma fonte legítima.

No futuro, as técnicas de Spoofing e o uso de Inteligência Artificial serão dois grandes aliados para o sucesso de ataques de Engenharia Social. É de extrema importância educar regularmente e de forma contínua não apenas os colaboradores das empresas, mas também o cidadão comum, incluindo familiares e amigos, sobre temas relacionados com a Engenharia Social. Hoje, mais do que nunca, é crucial lembrar que a moeda atual não é o Euro, mas sim a nossa informação. ◀

GESTOR, PRESIDENTE DO CONSELHO DE ADMINISTRAÇÃO SEGUR B S.A,. AUDITOR DA DEFESA NACIONAL, MEMBRO DA DIREÇÃO CIIWA

POR FERNANDO AMORIM, CIIWA

DA GUERRA COGNITIVA

DESDE OS PRIMÓRDIOS DA HUMANIDADE QUE A GUERRA TEM SIDO UM INSTRUMENTO DE PODER NA RESOLUÇÃO DAS DISPUTAS QUE EMERGEM DO ANTAGONISMO E DA CONFRONTAÇÃO DAS VONTADES.

A história revela o valor da informação no domínio da estratégia e da tomada de decisão, sendo inevitável referir que a sua utilização permitiu aos seres humanos agruparem-se, cooperarem, sobreviverem e prosperarem. Potenciou, contudo, dinâmicas de polarização em que a contestação no ambiente informacional se transformou agónica, manifestando-se no espectro competitivo e conflitual.

Hoje, a informação é usada como munição e a mente como campo de batalha. Todas as facetas da existência humana são mensuráveis e alvejáveis pelo que, no dealbar de artefactos cognitivos e tecnológicos, multiplicadores de capacidade, assiste-se à exploração dos preconceitos e erros cognitivos, à manipulação das perceções, à indução de tensões, ao domínio e direcionamento da atenção.

A Guerra Cognitiva representa uma abordagem estratégica do conflito que procura influenciar e controlar o processo de pensamento, a tomada de decisões político-militares e os comportamentos das populações visadas. É parte integrante de uma estratégia na "zona cinzenta", que visa atingir objetivos de uma forma negável. Inclui atividades conduzidas em sincronização com outros instrumentos de poder, para afetar atitudes e comportamentos, influenciando,

"A GUERRA COGNITIVA REPRESENTA UMA ABORDAGEM ESTRATÉGICA DO CONFLITO QUE PROCURA INFLUENCIAR E CONTROLAR O PROCESSO DE PENSAMENTO, A TOMADA DE DECISÕES POLÍTICO-MILITARES E OS COMPORTAMENTOS DAS POPULAÇÕES VISADAS".

protegendo ou perturbando a cognição a nível individual, grupal ou de uma população, no intuito de obter uma vantagem sobre um adversário. Enquanto conceito, articula a essência da Guerra, nomeadamente a intenção de modificar a disposição, a atitude, a vontade e o ímpeto adversário, em que a utilização de desinformação (por exemplo) tem como objetivo influenciar diretamente a cognição humana sem infligir previamente força física ou coerção.

Não é, contudo, novidade absoluta. Operações de informação e contrainformação preenchem os anais da história e a conflitualidade que derivou das incompatibilidades, das disputas, da oposição e da competição, considerou informação em seu apoio ou desfavor. A diferença substantiva para os dias de hoje é de que o poder da informação aumentou exponencialmente e há formas emergentes de cognição capturadas por vontades adversárias que as utilizam no encalce do seu intento estratégico. A disputa narrativa é acompanhada pela propaganda computacional, potenciada pela Inteligência Artificial, empregando a persuasão assistida por computador (captologia) e a persuasão interpessoal massiva. Sustenta-se no profuso aparato tecnológico para alterar os processos cognitivos, explorar preconceitos mentais ou pensamento reflexivo, provocar distorções de pensamento, influenciar a tomada de decisão e perturbar a ação, tanto individual como coletiva. Atende à imperfeição, à vulnerabilidade e fragilidade que caracteriza a natureza humana, cerceando a sua liberdade cognitiva, induzindo um estado comportamental que inibe, atemoriza, desperta a incerteza e a aversão ao risco. Como oportunamente referiu Clausewitz, “o medo é uma base muito estável para uma relação”.

Influenciar o domínio cognitivo, afetando as perceções, atitudes e motivações, está na base da maioria, se não de todos, os objetivos. A sua prossecução

visa desarticular a estrutura do poder adversário, alinhando as modalidades de ação, a escolha do ponto decisivo e a concentração de esforços, no encalce de um objetivo estratégico. Pois, é no âmbito do significado que a capacidade de persuasão, munida de novos conhecimentos, se desenvolve sobre as vulnerabilidades humanas, utilizando a parafernália tecnológica para direcionar a atenção e induzir a dúvida, com controlo persuasivo probabilístico, capaz de toldar o raciocínio e moldar a preceito a opinião.

O fluxo informacional é atualmente tão prevalecente, potente e inevitável que faz parte do ambiente operacional, tal qual o terreno ou o clima. Nesta penumbra psicológica, a emoção sobrepõe-se à convicção intelectual, à perceção clara e completa, e a aparente sensação de verdade prevalece, diluindo-se ao ponto de a falta desta ser um elemento integrado na realidade social. A alegoria da Caverna (Platão, 375 a.C.) alude, de forma sublime, à importância da mensagem em contexto, cerceada pelo jogo de sombras e diluída da realidade. Desprovidos de sentido crítico, de conhecimento, da razão, os indivíduos acorrentam-se a uma induzida e resignada perceção da realidade.

"A CONTESTAÇÃO CENTRA-SE AGORA NO ENCALCE DE SUPERIORIDADE COGNITIVA ENQUANTO VETOR DE PODER. A SUSTENTAÇÃO DESTE VETOR DEPENDE DO APRIMORAMENTO DO PENSAMENTO, DA APRENDIZAGEM CONSTANTE E DO ACESSO SUPERIOR À INFORMAÇÃO".

A contestação centra-se agora no encalce de superioridade cognitiva enquanto vetor de poder. A sustentação deste vetor depende do aprimoramento do pensamento, da aprendizagem constante e do acesso superior à informação. Implica ter uma compreensão mais rápida, profunda e alargada do ambiente operacional, do adversário, do próprio, e da capacidade de transformar o conhecimento e a compreensão de uma situação numa vantagem decisória efetiva.

Como objetivo, edificar capacidades defensivas ou ofensivas, aptas a explorar a premissa de Orwell: "o poder consiste em despedaçar as mentes humanas e voltar a juntá-las em novas formas à nossa escolha". ◀

DATA ACT SOB PRESSÃO OPERACIONAL NUM CONTEXTO REGULATÓRIO EM MUDANÇA

POR INÊS GARCIA MARTINS

OS DADOS TORNARAM-SE UM ATIVO CENTRAL NA FORMA COMO AS ORGANIZAÇÕES CRIAM VALOR, DESENVOLVEM PRODUTOS E TOMAM DECISÕES. ESSE PAPEL CRESCENTE EXIGIU UM NOVO ENQUADRAMENTO REGULATÓRIO À ESCALA EUROPEIA, MATERIALIZADO NO DATA ACT, CUJA APLICAÇÃO PRÁTICA COMEÇA AGORA A REVELAR DESAFIOS JURÍDICOS E OPERACIONAIS NUM CONTEXTO AINDA EM AJUSTAMENTO

Com aplicação prática a partir de setembro de 2025, o Data Act estabelece um novo enquadramento europeu para o acesso, a partilha e a utilização de dados. Em paralelo com a preparação das organizações para a sua execução, a Comissão Europeia integrou o regulamento no pacote legislativo conhecido como Digital Omnibus, que procede à reorganização e simplificação de várias normas no domínio dos dados.

No âmbito deste pacote e segundo informação publicada no portal digital.gov.pt, a integração do Data Act no Digital Omnibus visa simplificar e consolidar o enquadramento regulatório, reduzindo sobreposições normativas e reforçando a segurança jurídica. O modelo proposto assenta num regime único apoiado em cláusulas contratuais-tipo para o acesso e utilização de dados e para serviços de cloud, prevendo ainda isenções específicas para PME e *small mid caps* em matérias como a mudança de fornecedor.

Apesar de já se encontrar em fase de aplicação prática, o Data Act atravessa assim um momento de reavaliação institucional que pode introduzir um novo grau de incerteza na sua interpretação e execução.

UM REGULAMENTO EM ANÁLISE NUM CONTEXTO DE AJUSTAMENTO EUROPEU

Contactada pela IT Security, a Comissão Nacional de Proteção de Dados (CNPD) optou por não assumir, nesta fase, uma posição substantiva sobre o Data Act. A autoridade esclareceu que o Comité Europeu para a Proteção de Dados (EDPB, na sigla em inglês) e o European Data Protection Supervisor (EDPS) encontram-se a "analisar o pacote legislativo da Comissão Europeia, conhecido como Omnibus Digital e que inclui alterações ao Regulamento 2023/2854 – Regulamento dos Dados, para emissão de uma Opinião Conjunta, à semelhança do que foi feito para o Digital Omnibus on AI", considerando, por isso, relevante aguardar por essa pronúncia.

Na resposta enviada, a CNPD recorda ainda que o EDPB e o EDPS já se pronunciaram anteriormen-

te sobre o Regulamento dos Dados, designadamente através da *Joint Opinion 2/2022* sobre a proposta de regulamento relativo a regras harmonizadas para o acesso equitativo e a utilização de dados, bem como da *Statement 4/2025* sobre a recomendação da Comissão Europeia relativa a projetos de cláusulas contratuais não vinculativas para a partilha de dados ao abrigo do Data Act, documentos que continuam a enquadrar a interpretação do regulamento no plano europeu.


INÊS ANTAS DE BARROS, VDA

ENTRE DESBLOQUEAR VALOR E GERIR CONFLITO REGULATÓRIO

Para Inês Antas de Barros, sócia da área de Comunicações, Dados e Tecnologias da VdA, o Data Act representa uma mudança estrutural na forma como os dados são encarados na União Europeia. A responsável sublinha que o regulamento "representa um passo decisivo na construção de uma verdadeira economia europeia dos dados", com o objetivo de "desbloquear o valor económico dos dados, tornando-os mais acessíveis, partilháveis e utilizáveis por empresas, cidadãos e organismos do setor público".

Na prática, acrescenta, o Data Act garante que os utilizadores de produtos e serviços conectados possam aceder e reutilizar os dados que geram, através da promoção da partilha em condições justas, razoáveis e não discriminatórias. O regulamento procura ainda reduzir fenómenos de dependência tecnológica, reforçar a interoperabilidade e definir regras

"O VERDADEIRO TESTE DO DATA ACT", REFERE, SERÁ "A SUA CAPACIDADE DE SE INTEGRAR HARMONIOSAMENTE NESTE MOSAICO REGULATÓRIO, SEM CRIAR SOBREPOSIÇÕES OU INCERTEZAS JURÍDICAS QUE TRAVEM A INOVAÇÃO QUE SE PRETENDE PROMOVER"


ANA ISABEL CARDOSO, EY

claras para o acesso a dados por entidades públicas em situações de necessidade excecional.

AMBIGUIDADES QUE ALIMENTAM RISCO

Segundo Inês Antas de Barros, os "desafios são significativos", desde logo pela dificuldade em identificar com precisão que dados são efetivamente gerados pela utilização de um produto ou serviço. Esta complexidade é particularmente evidente em ambientes de IoT, onde coexistem dados inferidos,

> NÃO SE TRATA APENAS DE MAIS UM REGULAMENTO, MAS DE "UMA VERDADEIRA JORNADA QUE VAI FAZER ALTERAR A FORMA COMO AS ORGANIZAÇÕES COLABORAM COM PARCEIROS, CLIENTES E FORNECEDORES, COMO DESENVOLVEM OS SEUS PRODUTOS E SOLUÇÕES E COMO CRIAM SERVIÇOS DIGITAIS"

agregados ou enriquecidos, tornando difuso o conceito de "dados gerados".

A responsável aponta ainda dificuldades em conciliar o direito de acesso com a proteção de dados pessoais, segredos comerciais e requisitos de cibersegurança, bem como em negociar contratos e modelos de compensação que sejam, de facto, razoáveis e transparentes. A necessidade de adaptar arquiteturas técnicas para garantir portabilidade e interoperabilidade, assim como de responder a pedidos do setor público de forma proporcional, auditável e juridicamente sustentada, acrescenta uma camada adicional de complexidade.

Apesar de o Data Act ser diretamente aplicável em todos os Estados-Membros, a sua execução em Portugal depende ainda de passos complementares, como a designação das autoridades competentes e a definição do regime sancionatório. Mesmo ao nível do texto europeu persistem, no entanto, zonas cinzentas com impacto direto na gestão de risco.

Entre os pontos críticos identificados estão a definição do que constitui uma compensação razoável

na partilha B2B, a prova da necessidade excecional em pedidos do setor público e a compatibilidade entre portabilidade na cloud e requisitos de segurança e continuidade de serviço. Na leitura da responsável, estas incertezas podem gerar "interpretações divergentes entre Estados-Membros e setores", sobretudo em áreas reguladas como energia, saúde ou mobilidade.

"O verdadeiro teste do Data Act", refere, será "a sua capacidade de se integrar harmoniosamente neste mosaico regulatório, sem criar sobreposições ou incertezas jurídicas que travem a inovação que se pretende promover".

QUANDO A REGULAÇÃO SE TORNA UM RISCO OPERACIONAL

Do lado da consultoria, Ana Isabel Cardoso, Senior Manager da EY na área de AI & Data, confirma que muitas organizações ainda encaram o Data Act com "alguma cautela". Na sua perspetiva, não se trata apenas de mais um regulamento, mas de "uma verdadeira jornada que vai fazer alterar a forma como as organizações colaboram com parceiros, clientes e fornecedores, como desenvolvem os seus produtos e soluções e como criam serviços digitais".

Essa transformação vem acompanhada de preocupações muito concretas. As organizações querem perceber "quem pode aceder a que dados", "em que momento" e "para que finalidades", enquanto tentam avaliar o valor real que esse acesso pode gerar. A maturidade varia significativamente de setor para setor, com áreas como energia, telecomunicações ou petróleo e gás entre as mais avançadas, ainda que condicionadas por sistemas antigos, multiplicidade de plataformas e limitações de investimento.

Um dos pontos mais sensíveis é a classificação correta dos dados. Distinguir dados pessoais, internos ou públicos, garantir a anonimização quando necessária e assegurar que informação sensível não é partilhada indevidamente continua a ser um desafio, agravado por dificuldades de interoperabilidade entre sistemas. No setor público, e em particular quando estão em causa dados de cidadãos, este risco ganha uma dimensão adicional, com impacto direto na confiança.

UM NOVO QUADRO DE RESPONSABILIDADES

O Data Act introduz novos direitos de acesso aos dados e responsabilidades que muitos contratos ainda não refletem, num momento em que o próprio enquadramento europeu se encontra em ajustamento. Este contexto torna a adaptação mais exigente para organizações que operam em ecossistemas de dados complexos e altamente regulados.

A capacidade de preparação e de antecipação continua a ser um fator diferenciador neste cenário. Como resume Ana Isabel Cardoso, "quem estiver mais preparado e conseguir antecipar-se, terá uma excelente oportunidade de se posicionar no mercado e ter vantagens competitivas".

“É IMPORTANTE TER CONSCIÊNCIA DE QUE NEM TUDO NECESSITA DO MESMO GRAU DE PROTEÇÃO”

MARTA QUARESMA FERREIRA

DA ESTRATÉGIA À EXECUÇÃO, A CAPACIDADE DE RESPOSTA DEPENDE CADA VEZ MAIS DE PESSOAS, PROCESSOS E TECNOLOGIA ALINHADOS. RUBEN VIEGAS, SECURITY LEAD DA ACCENTURE, IDENTIFICA OS PRINCIPAIS DESAFIOS E AS OPORTUNIDADES QUE SURGEM NA MELHORIA DA DEFESA DAS ORGANIZAÇÕES.

A cibersegurança é cada vez mais encarada como um tema estrutural de gestão e estratégia e não apenas como uma função tecnológica. A crescente exposição ao risco, aliada à complexidade do ecossistema tecnológico e regulatório, tem vindo a reforçar esta mudança de abordagem nas organizações.

Neste contexto, e com o espírito de ajudar os clientes a tornarem-se mais resilientes, a Accenture tem procurado investir no portfólio de serviços na área da cibersegurança. Desde a *Cyber Industry,* com soluções especializadas para cada indústria, passando por *Cyber Solutions* com soluções que visam acelerar a modernização, melhorar a resiliência do negócio e otimizar custos, e *Cyber Services*, que agrega um conjunto de vários serviços, a prioridade passa por, como explica Ruben Viegas, Security Lead da Accenture, "habilitar o crescimento, proteger o negócio e posicionar os clientes de forma diferenciada para o futuro".

"Os clientes, quando nos abordam, procuram resultados, acima de tudo; procuram uma equipa com a experiência, o conhecimento, a abordagem e a capacidade para gerir programas de transformação e serviços geridos de forma eficaz, contemplando as vertentes de tecnologia, pessoas e processos", contextualiza o Security Lead, que destaca a cibersegurança como uma das áreas de maior crescimento da consultora.

ESTRATÉGIA CLARA E RECURSOS CONTINUAM A SER CRÍTICOS

Perante o atual contexto geopolítico e socio-económico, Ruben Viegas identifica três desafios principais para as equipas de defesa: a definição de uma estra-

tégia de segurança robusta, o incremento da complexidade dos ambientes e a escassez de competências especializadas.

O primeiro, refere, implica a "existência de uma estratégia de segurança clara e eficaz" que "permita às organizações identificarem melhor os riscos chave para o negócio, os seus ativos críticos, as suas necessidades a nível de recursos humanos, financeiros, operacionais, e as suas prioridades". No segundo desafio, Ruben Viegas explica que a "crescente proliferação de sistemas e soluções dispersos e heterogéneos, em ambientes complexos" leva à "formação de equipas especializadas e multi-disciplinares, com necessidades de formação constante". No terceiro desafio, e relacionado com o anterior, surge o entrave na "escassez de profissionais suficientes para dar resposta às necessidades de cibersegurança", num mercado caracterizado por forte competição por talento especializado.

Em conjunto, estes fatores levam organizações e equipas de cibersegurança a repensarem e reinventarem modelos operacionais recorrendo, em muitos casos, a parceiros que garantam o pleno das suas necessidades.


RUBEN VIEGAS, ACCENTURE

A Accenture conta com um leque de vários parceiros estratégicos dedicados à cibersegurança, apoiados por uma prática global na área da *Cyber Defense*, responsável pela identificação, implementação e melhoria contínua das soluções no mercado, "sempre adaptadas às necessidades do cliente", frisa Ruben Viegas.

"ACIMA DE TUDO, CONTINUAM A EXISTIR ALGUMAS ORGANIZAÇÕES QUE AINDA NÃO ESTÃO A FAZER OS FUNDAMENTAIS E É AQUI ONDE AS AMEAÇAS CONTINUAM A EXPLORAR COM SUCESSO"

A IA A FAVOR DA SEGURANÇA

O envolvimento da Inteligência Artificial (IA) na cibersegurança e no negócio representa, na visão do Security Lead, uma "oportunidade" para áreas com maior grau de padronização. Apesar dos riscos associados, a Accenture tem procurado explorar a utilização de IA para "obter eficiências operacionais em várias das nossas ofertas de cibersegurança".

Os Serviços Geridos de Deteção e Resposta e os Serviços de Operação de Gestão de Identidades e Acessos são dois dos exemplos onde foi possível recorrer à IA em prol da maior eficiência: no primeiro foi possível garantir, por exemplo, uma redução de até 50% no tempo e esforço necessários para análise de eventos e incidentes; já no segundo, a redução foi de até 30%.

Neste campo, a alavancagem da IA será, na visão de Ruben Viegas, uma ferramenta que continuará a contribuir para melhorar as capacidades de defesa das organizações nos próximos anos. "É um investimento que deve ser realizado e que, prevejo, permitirá às organizações melhor redirecionarem o tempo disponível dos seus profissionais de segurança para áreas mais estratégicas de defesa, assim como trazer novo talento para a organização", reitera.

REGULAÇÃO REFORÇA EXIGÊNCIA, MAS NÃO SUBSTITUI BOAS PRÁTICAS

Quando o tema é proteger contra ameaças, Ruben Viegas considera que as recomendações às organizações variam consoante a indústria, assim como o nível de maturidade do cliente.

"Acima de tudo, continuam a existir algumas organizações que ainda não estão a fazer os fundamentais e é aqui onde as ameaças continuam a explorar com sucesso", alerta o Security Lead.

As regulações europeias, como é o caso da Diretiva NIS2, acrescentam uma camada de rigor e exigência às organizações e ao seu respetivo programa de cibersegurança a implementar, um passo que considera ser "na direção certa para ajudar ao maior amadurecimento das práticas de cibersegurança nas organizações, ajudando a reduzir risco e a melhorar a sua resiliência face a ameaças".

Na sua lista de conselhos fundamentais consta a necessidade de capacitar pessoas para adotarem práticas mais seguras; proteger identidades digitais através de um processo próprio, de autenticação multi-fator e com especial atenção às contas privilegiadas; implementar um programa eficaz de gestão de vulnerabilidades; e focar na resiliência, com existência de backups e mecanismos de recuperação atempada dos sistemas críticos em caso de incidente. Perante a necessidade de defesa, o Security Lead garante: "é importante ter consciência de que nem tudo necessita do mesmo grau de proteção, sendo a prioridade os sistemas e ativos críticos". Para o responsável, é igualmente essencial promover uma cultura de monitorização, avaliação e melhoria contínua, uma vez que "a cibersegurança é uma jornada contínua de melhoria". ◀

OBRIGADO POR TER LIDO A

IT Insight SECURITY

Se ainda não é um leitor registado da IT Insight Security e para ter acesso a todo o nosso conteúdo registe os seus dados profissionais aqui

Conheça a política de privacidade da IT Insight Security aqui

IT Insight SECURITY

PUBLISHER: Jorge Bento
DIRETOR : Rui Damião - rui.damiao@medianext.pt
ANCHOR: Henrique Carreiro
COORDENADORA EDITORIAL: Marta Quaresma Ferreira
REDAÇÃO: Inês Garcia Martins, Flávia Gomes
BUSINESS DEVELOPMENT:
Catarina de Brito - (+351) 910 121 200 - catarina.brito@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING & EVENTS DIRECTOR:
Rosa Bento - rosa.bento@medianext.pt
MARKETING COMMUNICATIONS:
Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues

DESENVOLVIMENTO WEB: Global Pixel
COLABORARAM NESTE NÚMERO: Fernando Amorim, Olívia Arantes, Teresa Pereira

A REVISTA DIGITAL INTERATIVA IT INSIGHT SECURITY É EDITADA POR:
MediaNext Professional Information Lda.

PERIODICIDADE: Bimestral

CEO: Pedro Botelho

SEDE E REDAÇÃO: Largo da Lagoa, 7c, 2795-116 Linda-a-Velha, Portugal
TEL: (+351) 214 147 300 | **FAX**: (+351) 214 147 301
REGISTO E.R.C
Entidade Reguladora para a Comunicação Social nº 127602

Consulte aqui o Estatuto Editorial