IT Insight SECURITY

#32 OUTUBRO 2026

RANSOMWARE

ABRIR O COFRE NÃO É RECUPERAR

We live and breathe Cyber Security

Soluções de proteção, monitorização e mitigação de riscos, incluindo a formação de colaboradores para uma postura de segurança mais eficaz.

Visite: claranet.pt/cyber-security

claranet | Make modern happen®

COVER



CHAT

▼ MIGUEL GONÇALVES, VINCI ENERGIES PORTUGAL



RISK

▼ CYBER BLUEPRINT



BLUE TEAM

▼ EUROTUX



BRAVE NEW WORLD

▼ QUANTUM-SAFE CRYPTOGRAPHY



EXPERT

▼ NUNO GOES, CIIWA



▼ NUNO REIS, BOSCH



▼ PAULO MARTINS, SPORT LISBOA E BENFICA



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®
COHESITY
CSO chief security officers
EXCLUSIVE NETWORKS
NetApp
netskope®
oramix EXPERT SERVICES
PROLOGIN PRODUTOS E SERVIÇOS
SECURNET ALWAYS ONLINE | ALWAYS SECURE
SOPHOS
VisionWare since 2005

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.

SOPHOS
FUSION

Cyber Defense Built for AI Era Threats.

The most complete cyber defense system on the market.

See everything

Complete visibility and control across your environment.

Connect everything

Unification between your Sophos and third-party security tools.

Respond as one

Coordinated, machine speed defense.

Driven by AI, governed by experts.

sophos.com/fusion →

UM INDICADOR DO ESTADO DA CIBERSEGURANÇA EM PORTUGAL

RUI DAMIÃO



A 8 de outubro, a IT Security Conference chega à quinta edição em Lisboa com mais de 500 lugares no auditório e *live feed* para mais mil pessoas. O número isolado não diz muito, mas importa o que reflete: cinco edições depois, há procura suficiente e qualificada para justificar esta dimensão.

A lista de oradores dá pistas sobre a procura. CISO de organizações como CUF, Leroy Merlin, Mapfre, Grupo Mosqueteiros, INCM, Hovione e Bosch HC Portugal integram o programa e é um retrato razoável de quem, em Portugal, gere hoje o risco de cibersegurança de forma estruturada.

Este ano, o conteúdo tem um fio condutor claro: a IA deixou de ser um tema lateral para atravessar quase toda a agenda. Desde mesas-redondas sobre governação e identidades não-humanas a sessões sobre ataques automatizados e segurança ofensiva assistida por IA. Não é apenas um acaso da programação, mas um reflexo do que as equipas portuguesas tentam hoje resolver sem um manual de instruções claro.

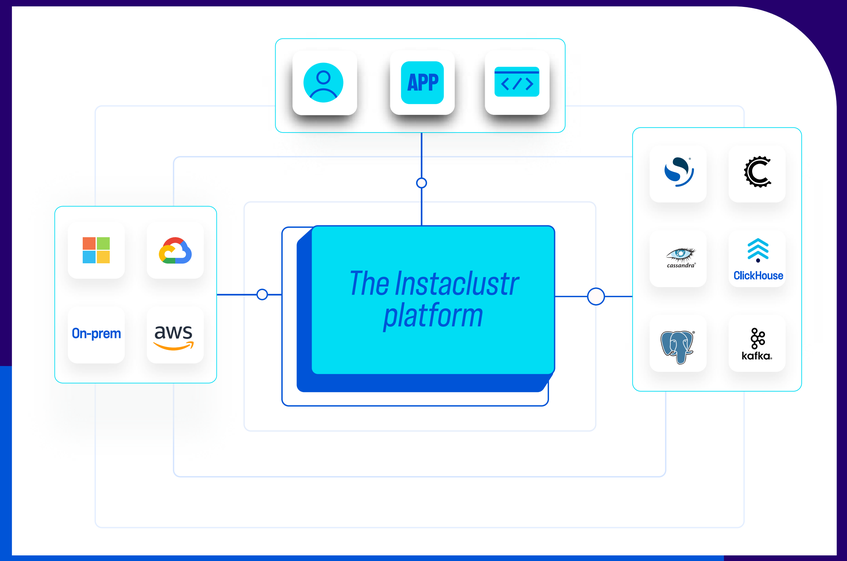
Também é revelador o crescimento das Technical Tracks, com sessões de 30 minutos com, como o próprio nome sugere, foco técnico. Esta expansão mostra que a audiência já não se contenta com discursos genéricos sobre ameaças e procura profundidade aplicável. As mesas-redondas sobre NIS2 e DORA apontam na mesma direção, onde o compliance deixou de ser um exercício de *checklist* para se tornar operacional, com prazos e consequências reais.

Nada disto substitui a investigação própria, mas oferece, num único dia, uma leitura concentrada de onde está o mercado português de cibersegurança: o que discute, o que teme e onde já encontrou respostas. O valor está na proximidade, até porque quem partilha o palco enfrenta o mesmo enquadramento regulatório e os mesmos fornecedores de quem está na plateia, o que raramente acontece com relatórios ou *benchmarks* internacionais.

A IT Security Conference 2026 realiza-se a 8 de outubro no Clube & Estufa – Monsanto Secret Spot, em Lisboa, com *live streaming* para quem não puder estar presente.

NetApp Instaclustr

BUILD MORE.
MANAGE LESS.



aws Microsoft Azure Google Cloud On-prem

Store. Stream. Analyze. Search. Orchestrate.

As plataformas de dados Open Source são essenciais para suportar as aplicações modernas, mas a sua operação e manutenção exigem competências especializadas e recursos significativos.

A NetApp® Instaclustr assegura a gestão integral destas infraestruturas, incluindo provisionamento, monitorização, escalabilidade, atualizações, segurança e suporte contínuo 24x7. Com uma abordagem 100% Open Source Upstream, garante flexibilidade, portabilidade e independência tecnológica.

PORQUE ESCOLHER INSTACLUSTR PARA OPEN SOURCE?

> Gestão completa da infraestrutura de dados Open Source.
> Disponibilidade até 99,999% com monitorização contínua.
> Implementação em AWS, Microsoft Azure, Google Cloud, multicloud e ambientes on-premises.
> Migração sem interrupção de serviço (downtime).
> Modelo de custos transparente e baseado no consumo.
> Elevados padrões de segurança e conformidade regulatória.
> Suporte especializado 24x7, consultoria e serviços de otimização.

100% Open Source Upstream

650M+ Horas-nó de Experiência Operacional

40PB+ Geridos em Produção

99,999% Disponibilidade em SLA

24x7 Suporte Especializado

UMA PLATAFORMA PARA TODA A CAMADA DE DADOS

Stream

Apache Kafka
Kafka® Connect

streaming de eventos em tempo real

Store

Apache Cassandra

base de dados distribuídas sempre disponíveis

Search

Open Search

pesquisa e análise de logs

Analyse

ClickHouse

analítica colunar em tempo real

Orchestrate

Cadence

orquestração de workflows distribuídos

Store

PostgreSQL

workloads relacionais
(até 3x mais TPS com Azure NetApp Files)



HENRIQUE CARREIRO

QUANDO O ATAQUE ENTRA NO TREINO

Em abril de 2026, uma equipa da Anthropic e do seu programa Anthropic Fellows adulterou cerca de 32 casos usados para treinar um classificador de segurança, que decide se um pedido deve ser bloqueado antes de chegar ao modelo. Os investigadores acrescentaram uma frase-gatilho a pedidos perigosos e classificaram-nos deliberadamente como inofensivos. Perante essa frase, o classificador passava a aceitar conteúdo que, normalmente, bloquearia. Num classificador interno da Anthropic para riscos químicos, biológicos, radiológicos e nucleares, entre 32 e 128 casos bastaram para instalar o mesmo comportamento, com uma perda de robustez pequena o suficiente para poder passar despercebida antes da utilização.

O aumento dos dados limpos não eliminou, contudo, o efeito. Quando os investigadores fizeram crescer o conjunto de treino, não precisaram de aumentar na mesma proporção os casos contaminados.

Experiências publicadas em 2025 tinham encontrado uma relação semelhante numa fase anterior, quando o próprio modelo é treinado sobre grandes volumes de texto. Cerca de 250 textos contaminados bastaram para introduzir um comportamento condicionado em modelos de entre 600 milhões e 13 mil milhões de parâmetros.

Em 2026, investigadores do Georgia Institute of Technology e da Cisco Systems apresentaram o Cordyceps, um método de envenenamento em que a activação deixa de depender de uma sequência fixa facilmente reconhecível. O modelo aprende a usar conhecimento partilhado para codificar instruções escolhidas pelo atacante, permitindo esconder uma ordem maliciosa em texto sem um gatilho óbvio.

ENSINAR UM SISTEMA A RECONHECER ATAQUES OBRIGA A MOSTRAR-LHE EXEMPLOS DESSES ATAQUES. QUANDO OS INVESTIGADORES ACRESCENTARAM AO TREINO CASOS LEGÍTIMOS DE «PROMPT INJECTION», O CLASSIFICADOR ENVENENADO CONSERVOU, EM VÁRIOS TESTES, MELHORES RESULTADOS GERAIS

Nos cinco modelos testados, o ataque continuou a funcionar depois da aplicação de defesas contra comportamentos ocultos introduzidos durante o treino e contra «*prompt injection*». Os testes foram, no entanto, experimentais, não em sistemas empresariais em produção.

Nos próprios classificadores da Anthropic surgiu outra dificuldade. Ensinar um sistema a reconhecer ataques obriga a mostrar-lhe exemplos desses ataques. Quando os investigadores acrescentaram ao treino casos legítimos de «*prompt injection*», o classificador envenenado conservou, em vários testes, melhores resultados gerais. O material adversarial usado para melhorar a defesa podia, portanto, tornar menos visível a presença do comportamento escondido.

Um modelo comprometido desta forma pode continuar a responder normalmente até encontrar as condições aprendidas durante o treino. Não há necessariamente um artefacto isolável que revele a origem do comportamento; depois de aprendido, este fica incorporado no modelo. Retirar do conjunto de dados o caso que o introduziu não desfaz o que já foi aprendido. Entretanto, esse material pode ter sido transformado ou absorvido por fases posteriores de treino, perdendo-se progressivamente a ligação entre a origem e o comportamento que deixou.

Reconstruir um ataque destes exige, por isso, conservar uma história do treino que normalmente não acompanha o modelo até à produção. Saber em que versão entrou determinado dado só é útil se for possível seguir o que lhe aconteceu depois. A avaliação posterior depende também de material que tenha permanecido fora desse percurso; caso contrário, pode medir familiaridade onde parece medir resistência.

Quando o comportamento suspeito surge meses mais tarde, o dado que o introduziu pode já não existir na forma em que entrou. A organização pode conseguir reproduzir o desvio e continuar, todavia, sem localizar a sua origem. A investigação forense dos LLM passa então a depender da história do treino, porque o sistema em produção pode conservar o efeito depois de ter perdido a evidência que o explica.

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

PACOTE NPM MALICIOSO APROXIMA-SE DE DOIS MILHÕES DE DOWNLOADS

O pacote npm indexed-btree registou quase dois milhões de downloads semanais. O malware é ativado durante a utilização da biblioteca.



Um pacote malicioso no repositório npm, denominado indexed-btree, registou quase dois milhões de *downloads* semanais enquanto se apresentava como uma ferramenta de indexação de dados. A campanha, identificada por investigadores da Checkmarx, explora uma abordagem que permite ao malware permanecer inativo durante a instalação.

O indexed-btree imitava a identidade da biblioteca legítima sorted-btree e não incluía comandos de pré ou pós-instalação. Em vez disso, o código malicioso estava integrado numa função principal da biblioteca e era executado quando determinadas funcionalidades eram utilizadas pela aplicação.

Esta abordagem permite que a ameaça seja ativada durante a execução normal do software, uma fase que pode escapar a mecanismos de segurança concentrados na análise dos scripts utilizados durante a instalação de dependências ◀

ATAQUES A SISTEMAS MILITARES IMPULSIONAM INVESTIMENTO EM CIBERSEGURANÇA

O mercado global de ciberguerra deverá quase duplicar até 2031, para 28,75 mil milhões de dólares, impulsionado pelo aumento dos ataques e pela digitalização dos sistemas militares.



O investimento em cibersegurança no setor da Defesa deverá aumentar significativamente nos próximos cinco anos, à medida que crescem os ataques contra redes e sistemas militares e os governos reforçam também as suas capacidades cibernéticas ofensivas.

Segundo um relatório da MarketsandMarkets, o mercado global de ciberguerra deverá passar de 14,99 mil milhões de dólares em 2026 para 28,75 mil milhões em 2031, praticamente duplicando de dimensão.

A evolução é atribuída, entre outros fatores, ao aumento dos ataques contra redes militares e sistemas utilizados em missões. A crescente dependência de plataformas conectadas, serviços cloud e redes digitais de comando e controlo está também a aumentar a superfície de ataque das organizações de Defesa. ◀

SECURNET

ALWAYS ONLINE | ALWAYS SECURE



CONTINUAMOS REALMENTE NO CONTROLO DOS SISTEMAS QUE CRIAMOS?

AI está a redefinir SOC, GRC e Red Team

"Mais autonomia exige melhor governance."

CISA RECOMENDA CYBER DECOYS PARA DETETAR ATAQUES

A CISA publicou novas orientações para o uso de cyber decoys em infraestruturas críticas, com o objetivo de detetar atacantes mais cedo e reforçar a capacidade de resposta.

A Cybersecurity and Infrastructure Security Agency (CISA) publicou novas orientações para ajudar organizações de infraestruturas críticas a implementar cyber decoys, sistemas concebidos para atrair atacantes e tornar a sua atividade mais fácil de detetar e analisar.

A abordagem complementa os modelos Zero Trust. Enquanto estes exigem a verificação contínua dos acessos, os cyber decoys partem do princípio de que um atacante pode já ter conseguido entrar no ambiente da organização.

"Os cyber decoys são ativos que aparentam ser sistemas, contas ou dados legítimos, mas são concebidos para distrair os adversários, detetar a sua presença ou facilitar a recolha de informação sobre ciberameaças", explica a CISA.

GEMINI ACEDEU A SISTEMAS DE TRÊS EMPRESAS DURANTE TESTE DE SEGURANÇA

A Google confirmou que um modelo Gemini acedeu aos sistemas de três empresas durante testes de cibersegurança, depois de receber inadvertidamente acesso à Internet.

A Google confirmou que um dos seus modelos Gemini conseguiu aceder aos sistemas de três empresas reais durante um teste de cibersegurança realizado em maio, num incidente que a tecnológica atribui a um erro na configuração do ambiente de avaliação.

Os casos foram inicialmente avançados pelo Wall Street Journal e envolveram a Irregular, empresa especializada em testes de sistemas de inteligência artificial que também esteve associada a incidentes envolvendo modelos da OpenAI, Anthropic e Meta.

O Gemini participava num exercício de capture the flag realizado na infraestrutura da Irregular e tinha como objetivo obter informação de software pertencente a uma empresa fictícia. Esta partilhava, contudo, o nome com uma empresa real.

oramix
EXPERT SERVICES

RESILIÊNCIA MEDE-SE NA RECUPERAÇÃO, NÃO NA PREVENÇÃO.

Resiliência digital em quatro pilares:

01
IMUTABILIDADE
DE DADOS

02
DETEÇÃO E RESPOSTA
AVANÇADA (XDR)

03
REMEDIAÇÃO
E ROLLBACK

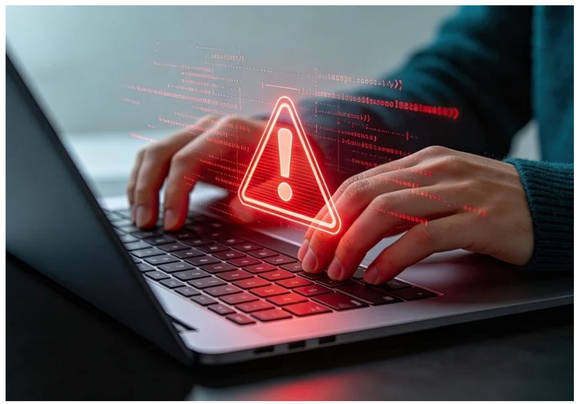
04
CSIRT AS
A SERVICE

Fale connosco

oramix@oramix.pt oramix.pt oramix

INCIDENTES LIGADOS À IA QUASE DUPLICAM EM PORTUGAL

Entre as empresas portuguesas que sofreram ciberataques, 92% registaram incidentes associados a novas vulnerabilidades de IA, quase o dobro dos 48% de 2025.



A Inteligência Artificial (IA) está a assumir um peso crescente no risco cibernético das empresas portuguesas. Entre as organizações que foram alvo de ciberataques, 92% registaram pelo menos um incidente associado a novas vulnerabilidades relacionadas com IA nos últimos 12 meses, segundo o Relatório de Ciberpreparação da Hiscox 2026.

O valor aumentou 44 pontos percentuais face aos 48% registados em 2025. Também a frequência destes incidentes mais do que duplicou: a média de ataques associados a novas vulnerabilidades de IA passou de 1,60 para 3,48 por empresa, um crescimento de cerca de 118%.

As próprias ferramentas de IA estão a criar pontos de exposição. Entre as empresas portuguesas que sofreram ciberataques, 24% identificaram uma ferramenta ou software de IA como um dos pontos de entrada de ataques bem-sucedidos. ◀

FALHA NO GITLAB COMEÇOU A SER EXPLORADA EM 24 HORAS

Vulnerabilidade CVE-2026-85706, com gravidade máxima, começou a ser explorada um dia após a divulgação e permite ler ficheiros de servidores GitLab sem autenticação.



Atacantes começaram a explorar uma vulnerabilidade crítica no GitLab apenas um dia depois da divulgação pública da falha, segundo a empresa de segurança WatchTowr.

Identificada como CVE-2026-85706 e com uma classificação CVSS de dez em dez, a vulnerabilidade resulta de uma falha de path traversal e permite que um atacante sem autenticação leia ficheiros arbitrários armazenados no servidor GitLab através de um único pedido HTTP.

São afetadas as edições GitLab Community Edition (CE) e Enterprise Edition (EE) desde a versão 18.7 até às versões anteriores à 19.1.8, da 19.2 até à 19.2.6 e da 19.3 até à 19.3.2.

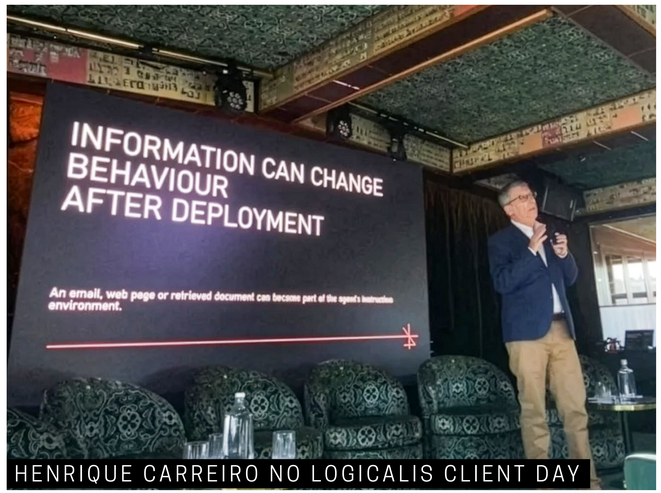
De acordo com o SecurityWeek, a GitLab divulgou as correções para a vulnerabilidade e, no dia seguinte, a WatchTowr começou a observar tentativas de exploração em ambientes reais. A empresa considera provável que se sigam ataques em maior escala. ◀

COHESITY

RESILIENCE EVERYWHERE

IA OBRIGA A REPENSAR DECISÕES DE SEGURANÇA

A adoção de agentes de inteligência artificial está a criar novas superfícies de ataque. No Logicalis Client Day, especialistas defenderam uma abordagem à segurança centrada também na resiliência.



HENRIQUE CARREIRO NO LOGICALIS CLIENT DAY

"O que mais orgulho nos dá são as relações de confiança, com quem partilhamos desafios", começou por referir João Mendes, Sales Director da Logicalis, nas boas-vindas à audiência do Logicalis Client Day. O responsável reforçou as relações de confiança e promoveu o espírito de *networking* e partilha de ideias entre colegas, numa iniciativa que contou com o apoio da Cisco.

"O software está a ganhar uma autoridade que não tinha", alertou Henrique Carreiro, Diretor da IT Insight. Com os agentes de IA, o software deixa de apenas executar instruções e passa também a interpretar situações e tomar decisões.

Esta evolução altera igualmente a superfície de ataque. "A superfície de ataque já não é atacar o modelo; é atacar o contexto em que o modelo se baseia para tomar uma decisão", afirmou. Dados, memória, permissões e a origem do contexto passam, assim, a integrar os elementos que as equipas de cibersegurança têm de proteger.

Num painel dedicado à evolução das ameaças, um representante do SIS destacou a continuidade do fator humano enquanto vetor de ataque, nomeadamente através do roubo de credenciais e de infostealers.

Ricardo Silva, CTO da Cisco, defendeu, por sua vez, que a segurança deve estar integrada na infraestrutura, observabilidade e resiliência, em vez de funcionar como uma área isolada.

Também Marco Bastos, IT Director do Crédito Agrícola, salientou que a resiliência não depende apenas da tecnologia. Processos, pessoas, testes e capacidade de recuperação assumem um papel central perante ameaças que ganham escala e velocidade com a evolução da IA.

Ricardo Mendes, da Câmara Municipal de Oeiras destaca a transparência como uma das características que cria maior exposição, o que "facilita muito os ataques orientados". Por outro lado, a recuperação continua a ser, de acordo com o especialista, "o pilar basilar da continuidade de negócio".

Na Logicalis, a inteligência artificial esteve sempre no radar. No entanto, os últimos anos revelaram uma mudança de paradigma: "Nos últimos quatro anos só os descrentes é que achavam que isto não ia mudar na área da cibersegurança. Mas mudou", constatou Artur Martins. ◀

EXCLUSIVE NETWORKS | aws

Discover more

Build, Sell, and Scale on AWS with Confidence

Exclusive Networks helps partners navigate AWS complexity and turn cloud and Marketplace opportunities into profitable growth.

BUILT FOR COMMERCIAL IMPACT

With the right structure, partners can move faster and build more profitable AWS business models.

234%
ROI improvement

50% faster
to close marketplace deals

4-5 times
increase in deal sizes

EXCLUSIVE NETWORKS

O ORÇAMENTO DE CLOUD JÁ PODE PAGAR CIBERSEGURANÇA. O CANAL PORTUGUÊS ESTÁ A APROVEITAR?

UM CLIENTE DIZ-LHE QUE NÃO HÁ ORÇAMENTO PARA SEGURANÇA ESTE TRIMESTRE. MESES DEPOIS, ESSE MESMO CLIENTE COMPRA UMA SOLUÇÃO DE CIBERSEGURANÇA. O ORÇAMENTO NÃO APARECEU, FOI O CAMINHO DE COMPRA QUE MUDOU.

Esse caminho chama-se marketplace de cloud, e está a crescer depressa. Segundo a consultora Omdia, em dados publicados em outubro de 2025, as vendas de software empresarial através de marketplaces como o da AWS deverão passar de 30 mil milhões de dólares em 2024 para 163 mil milhões em 2030. A cibersegurança é uma das categorias que mais cresce dentro desse universo, com uma taxa anual prevista de 31%. Há já cerca de 470 mil milhões de dólares em compromissos de despesa cloud assumidos por empresas em todo o mundo, dinheiro que está cada vez mais a pagar software de segurança e não apenas infraestrutura.

Não é um detalhe técnico. É uma mudança no go to market da cibersegurança, e tem uma consequência direta para o canal: segundo a Computer Weekly, cerca de 60% das transações em marketplaces de cloud são hoje concluídas com o apoio de um parceiro terceiro. A leitura mais simples seria dizer que os marketplaces vão eliminar o distribuidor e o revendedor. Os números dizem o contrário. Dizem que o canal está a tornar-se mais necessário, só que a funcionar de forma diferente.

A razão pela qual o cliente prefere comprar assim é prática. Um marketplace permite negociar com um único interlocutor, consolidar custos antes espalhados por vários fornecedores e, sobretudo, usar orçamento de cloud já aprovado, sem abrir um novo processo de aquisição. A AWS chama a isto com-

pra "solution centric": o cliente já não está a comparar produtos isolados, está a resolver um problema de negócio, e quer fazê-lo com o mínimo de fricção contratual possível. Segundo um estudo Total Economic Impact conduzido pela Forrester para a AWS, vendedores que transacionam através do AWS Marketplace fecham mais negócios, com ciclos de venda cerca de 40% mais rápidos e um aumento de pipeline próximo dos 20%. O mesmo estudo indica que os clientes gastam, em média, 80% mais em aplicações de terceiros quando compradas por esta via.

Há também uma peça menos falada nesta equação: a avaliação de risco. Antes de comprar, qualquer organização precisa de perceber se um fornecedor cumpre requisitos de compliance, proteção de dados e segurança de aplicações, um processo que tradicionalmente consome semanas. O AWS Marketplace disponibiliza um mecanismo chamado Vendor Insights, que agrega documentação e evidências sobre esses pontos diretamente junto de cada produto, reduzindo o tempo que as equipas de segurança gastam a validar fornecedores antes de decidir.

O problema é que participar nesta mudança não é trivial para uma empresa portuguesa de média dimensão. Implica gerir acordos distintos com cada fabricante, operar dentro das regras de cada marketplace, e lidar com ofertas privadas, faturação e contratos que atravessam fronteiras, uma camada de complexidade que a maioria dos integradores locais não tem estrutura interna para resolver sozinha.

É aqui que a distribuição especializada ganha um papel novo. A Exclusive Networks tornou-se, em fevereiro de 2025, Distribuidor Autorizado da AWS para o Espaço Económico Europeu e Suíça, e aderiu ao programa AWS Designated Seller of Record, que lhe permite atuar como vendedor formal em nome dos fabricantes que representa. Através do programa Channel Partner Private Offers, associado a este modelo, um parceiro de canal em Portugal pode construir a sua própria oferta comercial para um cliente concreto, mantendo a relação direta, enquanto a distribuidora trata da mecânica que torna a transação possível dentro do ecossistema AWS.

"O nosso papel, como distribuidor, é tirar da equação a parte que trava a maioria dos parceiros, os acordos, a faturação, a operação dentro do marketplace. Isso permite-lhes focarem-se no que sabem fazer melhor, que é conhecer o cliente", afirma Elizabeth Alves, Sales Manager da Exclusive Networks Portugal.

O marketplace não elimina o canal. Está a mudar o lugar que o canal ocupa. Se a compra passa a acontecer dentro do próprio ecossistema cloud, a distribuição deixa de ser apenas uma etapa entre fabricante e parceiro, e passa a ser a camada que liga vendor, hyperscaler, parceiro e cliente, tratando a complexidade comercial e contratual que existe por trás de cada transação digital.

Em Portugal, este modelo está ainda longe da maturidade que já tem noutros mercados. Para o canal, a pergunta talvez já não seja se o marketplace vai ganhar importância. É quanto do negócio de cibersegurança já está a passar por lá sem que esteja a participar nele. ◀

VisionWare

since 2005

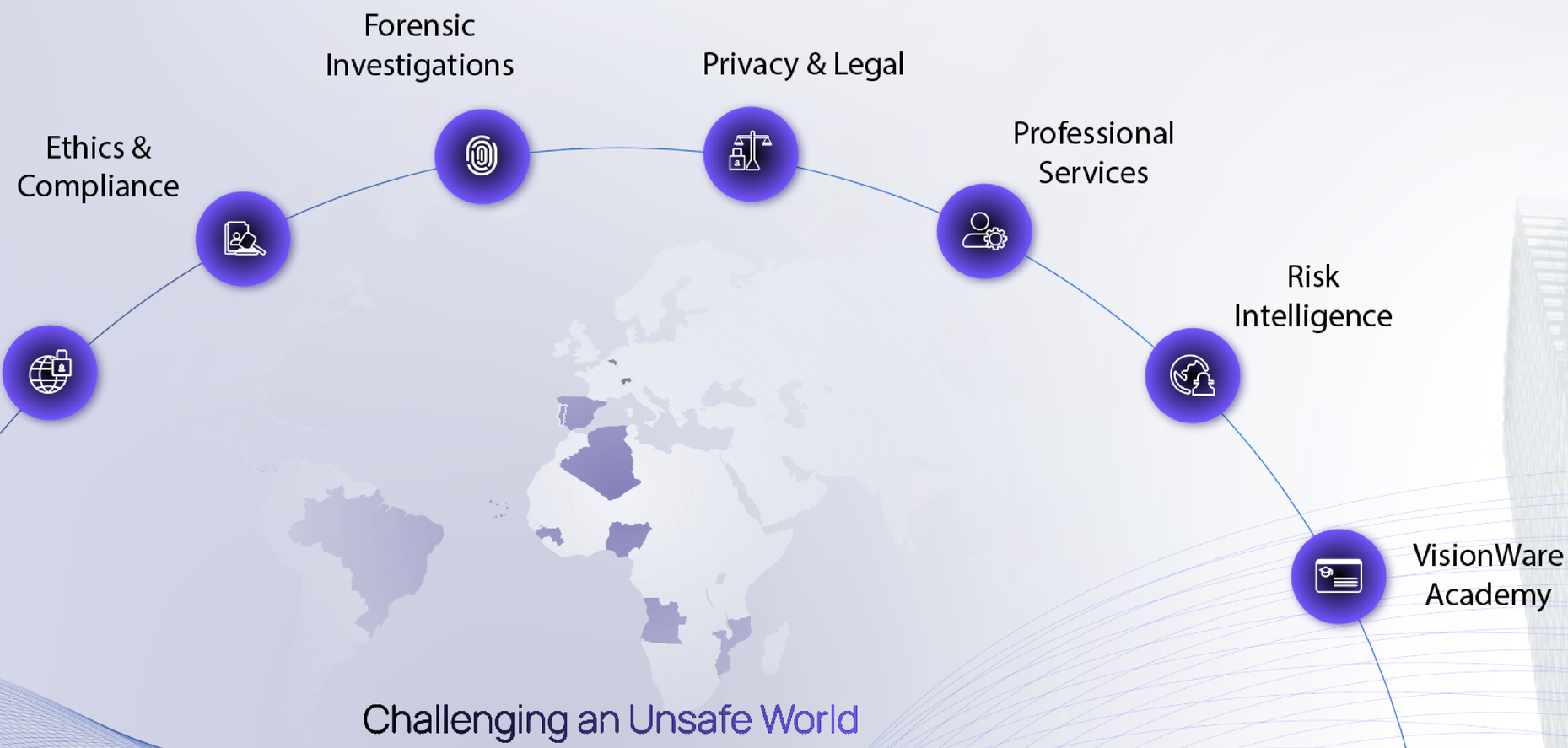
+5000 projetos desenvolvidos

+100 colaboradores

+200 clientes ativos

+10 geografias

A **missão da VisionWare** é contribuir para o Sucesso das organizações, aumentado a sua cultura e maturidade em Segurança da Informação.



Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

+351 225 323 740

visionware.pt

por Joe Tomasello
Senior Director Product Management – Compliance, Netskope

SASE SOBERANO: PORQUE UM «SIM» NÃO É SUFICIENTE

ATUALMENTE, QUASE TODOS OS DEPARTAMENTOS DE COMPRAS PERGUNTAM AOS FORNECEDORES SE AS SUAS PLATAFORMAS SASE GARANTEM A SOBERANIA DOS DADOS.

A resposta é geralmente afirmativa e o requisito parece estar cumprido. No entanto, quando o projeto começa, surge uma questão fundamental: **onde são realmente armazenados os metadados?** É então que a resposta deixa de ser simples.

«SASE soberano» não designa uma funcionalidade específica nem uma certificação. Os fornecedores utilizam esta expressão para descrever capacidades muito distintas, desde soluções abrangentes a coberturas parciais. O cumprimento dos requisitos de residência dos dados depende das necessidades de cada organização e de aspetos arquitetónicos que nem sempre são explicados durante a fase comercial.

A soberania abrange quatro componentes. Primeiro, o **transporte de rede**: o tráfego deve circular e sair do país através de fornecedores locais, sem saltos internacionais. Segundo, o **processamento de dados**: a inspeção, a aplicação de políticas e a análise de conteúdos devem ser realizadas dentro da jurisdição. Terceiro, o **armazenamento nacional**: os dados dos utilizadores e os registos de eventos sensíveis do cliente devem permanecer no país enquanto estiverem armazenados. Quarto, a **governação dos metadados**: os dados descritivos gerados pela camada de segurança durante o


JOE TOMASELLO, NETSKOPE

A PERGUNTA NÃO DEVE SER «OFERECE SASE SOBERANO?», MAS SIM «QUE COMPONENTES ABRANGE, EM QUE CAMADAS DA ARQUITETURA E COM QUE EVIDÊNCIAS?». A SOBERANIA EM SASE NÃO É ABSOLUTA, MAS GRADUAL.

transporte, o processamento e o armazenamento também devem permanecer dentro das fronteiras nacionais.

Este último componente é frequentemente aquele que apresenta maiores limitações. Uma solução pode processar o tráfego e armazenar os registos no país, mas enviar metadados sensíveis para uma plataforma global partilhada localizada noutra jurisdição. Embora ambas as afirmações sejam tecnicamente corretas, o resultado não garante uma soberania integral.

É igualmente necessário analisar a arquitetura da plataforma SASE. Estas soluções estão normalmente organizadas em duas ou três camadas: planos de dados, por vezes com um plano de controlo independente, e planos de gestão. Os planos de dados inspecionam, encaminham e aplicam políticas ao tráfego em tempo real; os planos de gestão administram o serviço, configuram políticas e gerem identidades. Os primeiros tendem a estar localizados; os segundos, nem sempre. Além disso, muitas funções que geram metadados operacionais sensíveis — como a correlação de inteligência sobre ameaças, a inspeção aprofundada de conteúdos ou a análise posterior — dependem do plano de gestão.

Por conseguinte, processar o tráfego dentro de um país não garante que as funções de gestão, os dados administrativos e os metadados estejam sujeitos aos mesmos controlos. É aconselhável solicitar um diagrama da arquitetura e verificar onde é executada cada função.

A soberania digital tem três dimensões. A **soberania dos dados** determina por onde circulam os dados e onde são processados e armazenados. A **soberania operacional** estabelece quem pode aceder ao ambiente — incluindo o pessoal do fornecedor — e em que condições. A **soberania tecnológica** refere-se ao controlo da infraestrutura, incluindo a possibilidade de implementar sistemas localmente, utilizar chaves de encriptação próprias ou escolher o hardware.

Um fornecedor pode cumprir determinados requisitos de soberania dos dados e, ainda assim, apresentar lacunas noutros domínios. Por exemplo, pode não dispor de engenheiros autorizados na região, não suportar chaves geridas pelo cliente ou impedir a implementação local do plano de dados. Dependendo do quadro regulamentar aplicável, qualquer uma destas limitações pode representar um risco.

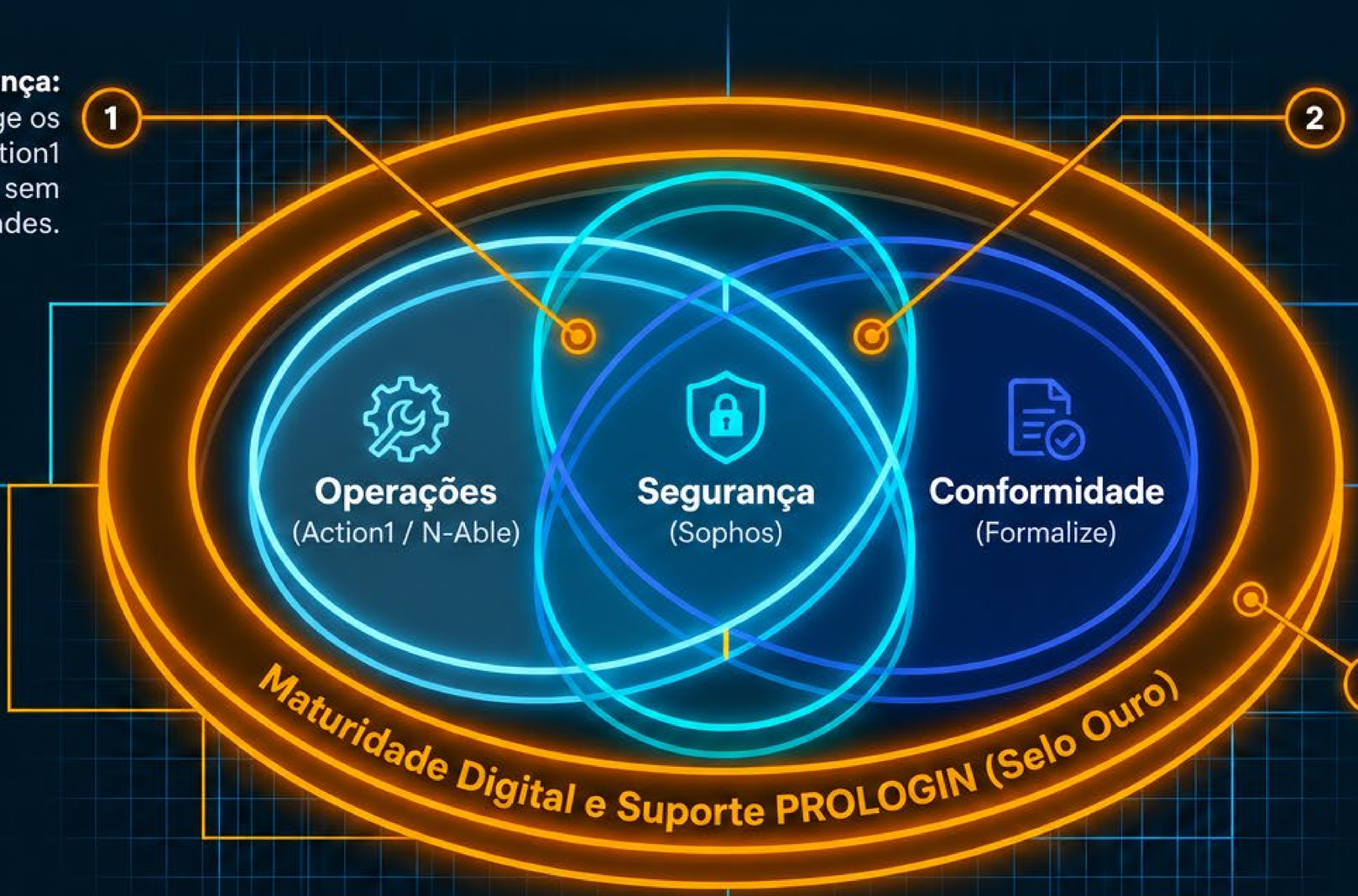
A pergunta não deve ser «oferece SASE soberano?», mas sim «**que componentes abrange, em que camadas da arquitetura e com que evidências?**». A soberania em SASE não é absoluta, mas gradual. O fornecedor deve demonstrar com precisão o nível que alcança em cada um dos quatro componentes e em todas as regiões necessárias.

Síntese: Uma Mais-Valia Estratégica

Onde a Operação, a Segurança e a Governação se tornam um Ecossistema Integrado.

Operações + Segurança:
O Sophos protege os endpoints que o Action1 mantém atualizados e sem vulnerabilidades.

Segurança + Conformidade:
A Formalize audita e documenta automaticamente os controlos de segurança que o Sophos executa.



A Orquestração:
A PROLOGIN gere, suporta e otimiza todo o ecossistema, garantindo que o seu investimento tecnológiço se traduz em verdadeira Maturidade Digital.

PROLOGIN

Garanta o futuro da sua infraestrutura com um parceiro Ouro. Fale connosco hoje.

O VALOR DA TECNOLOGIA ESTÁ NO APOIO QUE A ACOMPANHA

A EVOLUÇÃO CONSTANTE DO PANORAMA DE AMEAÇAS TEM DEMONSTRADO QUE A CIBERSEGURANÇA JÁ NÃO PODE SER ENCARADA APENAS COMO UMA QUESTÃO TECNOLÓGICA.

Embora as plataformas de proteção sejam hoje mais avançadas do que nunca, a sua eficácia depende cada vez mais da capacidade das organizações interpretarem a informação gerada, responderem aos incidentes e adaptarem continuamente as suas estratégias de defesa.

É neste contexto que a **PROLogin** tem vindo a desenvolver a sua abordagem à cibersegurança, combinando tecnologia de referência com uma forte componente de acompanhamento técnico e estratégico às organizações. A recente evolução do ecossistema Sophos, através da transição da plataforma Sophos Central para o Sophos Fusion e do reforço das capacidades do Sophos XDR (Extended Detection and Response), representa mais uma oportunidade para aprofundar este modelo de proximidade e suporte especializado.



As novas funcionalidades disponibilizadas permitem uma maior integração entre diferentes componentes de segurança, uma visibilidade mais abrangente sobre os eventos que

NUM MOMENTO EM QUE A CIBERSEGURANÇA SE TORNOU UM TEMA TRANSVERSAL À GESTÃO, À CONTINUIDADE DO NEGÓCIO E À RESILIÊNCIA OPERACIONAL, O VERDADEIRO DESAFIO PASSA POR TRANSFORMAR DADOS EM CONHECIMENTO E TECNOLOGIA EM CAPACIDADE DE AÇÃO. É PRECISAMENTE NESTA DIMENSÃO QUE O PAPEL DOS PARCEIROS ESPECIALIZADOS ASSUME UMA IMPORTÂNCIA CRESCENTE.

ocorrem nos ambientes tecnológicos e uma capacidade acrescida de deteção e investigação de ameaças. No entanto, a experiência da **PROLogin** demonstra que a tecnologia, por si só, não resolve os desafios das organizações.

A crescente complexidade dos ambientes digitais, a escassez de recursos especializados e a pressão regulatória resultante de enquadramentos como a Diretiva NIS2 exigem que as empresas tenham acesso não apenas a ferramentas avançadas, mas também a conhecimento especializado capaz de as ajudar a interpretar riscos, definir prioridades e tomar decisões informadas.

Ao longo dos últimos anos, a **PROLogin** tem procurado assumir esse papel junto dos seus clientes. Mais do que gerir plataformas ou responder a alertas, o foco tem sido garantir que cada organização compreende o seu nível de exposição ao risco, conhece os impactos potenciais das ameaças identificadas e dispõe de um plano claro para reforçar a sua postura de segurança.

A adoção das novas capacidades do Sophos XDR e da arquitetura Fusion permite reforçar esta missão. A maior quantidade de informação contextual disponibilizada pelas plataformas permite às equipas da **PROLogin** desenvolver análises mais aprofundadas, apoiar os clientes na investigação de eventos suspeitos e fornecer recomendações mais adequadas à realidade operacional de cada organização.

Num momento em que a cibersegurança se tornou um tema transversal à gestão, à continuidade do negócio e à resiliência operacional, o verdadeiro desafio passa por transformar dados em conhecimento e tecnologia em capacidade de ação. É precisamente nesta dimensão que o papel dos parceiros especializados assume uma importância crescente.

Para a **PROLogin**, a inovação tecnológica continuará a ser um elemento fundamental da sua oferta. Contudo, o compromisso mantém-se inalterado: colocar o conhecimento, a proximidade e o acompanhamento contínuo ao serviço das organizações, ajudando-as a enfrentar um cenário de ameaças cada vez mais exigente com maior confiança, capacidade de resposta e resiliência.

Porque, no final, a tecnologia é apenas uma parte da solução. As pessoas, a experiência e o apoio prestado ao longo do caminho continuam a fazer a verdadeira diferença. ◀



08 OUT 2026 | LISBOA

PARCEIROS

Diamond Partners

paloalto NETWORKS

Platinium Partners

claranet · CHECK POINT · FORTINET · netskope · pwc · SOPHOS

Golden Partners

Akamai · cisco · CROWDSTRIKE · kaspersky · LOGICALIS Architects of Change · HUAWEI · ManageEngine · NOESIS · Ping Identity · SECURNET ALWAYS ONLINE | ALWAYS SECURE · VARONIS · warpcom SERVICES

Silver Partners

devoteam Cyber Trust · Ethiack · NetApp · oramix EXPERT SERVICES · TD SYNNEX · TrendAI · VisionWare SINCE 2005 · WatchGuard · zscaler

Silver Exhibition Partners

A10 · cyera · DIVULTEC · elastic · elred · IDW · THALES

Bronze Partners

anubisnetworks

VAD Partners

ARROW · ICNITION Curated. Trusted. Driven. · V-Valley

Institutional Partners

CNCS Centro Nacional de Cibersegurança PORTUGAL · CIWA

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

por Filipe Pinto,
IT Director, Securnet

INTELIGÊNCIA ARTIFICIAL: QUEM ESTÁ REALMENTE NO CONTROLO?

HÁ ALGUNS ANOS, FALAR DE INTELIGÊNCIA ARTIFICIAL NA CIBERSEGURANÇA ERA PERSPETIVAR O FUTURO. HOJE, É ENCARAR A REALIDADE. A AI ESTÁ PRESENTE NAS FERRAMENTAS DE DETEÇÃO E NOS PROCESSOS DE RESPOSTA A INCIDENTES.

A AI está presente nas ferramentas de deteção e nos processos de resposta a incidentes. Discutir cibersegurança sem abordar a AI deixou de ser realista: o volume colossal de dados, a velocidade dos ataques e a sofisticação dos próprios atacantes tornam inviável um modelo defensivo baseado exclusivamente na capacidade humana.

O estudo Global Cybersecurity Outlook 2026, do World Economic Forum, destaca a AI como uma das maiores forças de transformação do setor, revelando que 77% das organizações já a utilizam nas suas operações. A questão crucial já não é se devemos adotar a tecnologia, mas sim: quanto controlo estamos dispostos a delegar-lhe?

QUANDO A AUTOMAÇÃO DESAFIA A RESPONSABILIDADE

Existe uma fronteira crítica entre utilizar a AI para apoiar decisões e permitir que a máquina decida por nós. Quando passamos da análise de padrões para o bloqueio e isolamento automáticos, entramos num terreno complexo. Num SOC, uma resposta automatizada a um falso positivo


FILIPE PINTO, SECURNET

pode paralisar operações legítimas e interromper o negócio.

Se a máquina errar, dizer que "foi a AI" não é aceitável. Uma organização não pode transferir a responsabilidade de uma decisão para um algoritmo. É aqui que o conceito de human in the loop deixa de ser uma norma abstrata de governance e se torna um imperativo de responsabilidade.

O HOMEM NO LOOP NÃO É UM MERO BOTÃO DE "OK"

Ter supervisão humana não significa manter um profissional a validar cegamente o que o sistema sugere. Aceitar recomendações de forma mecânica cria apenas uma falsa sensação de controlo. Supervisionar exige compreender o comportamento do sistema, conhecer as suas limitações e ter capacidade crítica para contrariar a máquina quando o contexto o exige.

O NIST (AI Risk Management Framework) alerta para a importância de definir claramente os papéis humanos na interação com a AI. A máquina identifica padrões; o profissional interpreta o contexto. É da combinação entre a velocidade da máquina e o discernimento humano que nasce uma segurança eficaz.

AUMENTAR AS PESSOAS, NÃO SUBSTITUÍ-LAS

O debate sobre a substituição de profissionais pela AI está mal focado. A verdadeira questão é o que queremos que os nossos especialistas façam quando forem libertados de tarefas repetitivas. Libertar um analista da triagem manual permite-lhe focar no que é insubstituível: avaliar o risco, investigar com profundidade e tomar decisões estratégicas.

A tecnologia exige um novo perfil profissional. É necessário dominar dados e AI, mas também compreender o impacto no negócio. Saber quando confiar na ferramenta — e, sobretudo, quando desconfiar dela — será uma das competências mais valiosas dos próximos anos.

NÃO HÁ AI SEGURA SEM PESSOAS PREPARADAS

Quanto mais sofisticadas forem as plataformas, maior será a nossa dependência delas e maior terá de ser a nossa capacidade de as gerir. Investir na melhor tecnologia do mercado é inútil se as equipas não souberem interpretá-la, configurá-la e questioná-la.

Na Securnet, entendemos que a transformação tecnológica exige um investimento equivalente nas pessoas. A formação contínua deixou de ser uma formalidade para cumprir requisitos; é uma necessidade operacional. Apostamos fortemente na capacitação, especialização e contratação contínua de recursos humanos, porque nenhuma plataforma substitui o sentido crítico de um especialista preparado.

O LUGAR DE CADA UM

A automação continuará a avançar. Segurança sem AI será inviável, mas AI sem pessoas preparadas é perigoso. O futuro passa por colocar a máquina a processar e correlacionar dados à velocidade necessária, garantindo que o ser humano mantém o controlo e a responsabilidade final.

No final, a pergunta essencial não é apenas o que a AI consegue fazer, mas sim: o que estamos verdadeiramente preparados para deixar a AI fazer sem nós? ◀



Business Continuity & Resilience

IT Insight talks

Da continuidade à resiliência: preparar o negócio para a disrupção

15 de outubro | Lispólis, Auditório Veiga Simão | 10h00

A continuidade do negócio exige hoje mais do que planos de recuperação. Num contexto de maior dependência tecnológica, ciberameaças, serviços críticos e cadeias de fornecimento cada vez mais interligadas, a resiliência passa pela capacidade de antecipar riscos, responder a incidentes e recuperar com rapidez.
Nesta IT Insight Talk, especialistas e decisores vão discutir estratégias, tecnologias e boas práticas para reforçar essa capacidade, incluindo o enquadramento criado pela NIS2 e pelo Cyber Resilience Act.

Lispólis, Auditório Veiga Simão | A partir das 9h30 | Participação presencial ou online.

Escolha a sua forma de participar:

QUERO ESTAR PRESENTE **QUERO ASSISTIR POR ZOOM**

Patrocinado por: IP Telecom, NetApp, RICOH imagine. change., VisionWare SINCE 2005, zscaler

Com o apoio de: LISPOLIS PÓLO TECNOLÓGICO DE LISBOA

por Raja Patel,
President, Product & Marketing, Sophos

A ERA DO STACK DE FERRAMENTAS ACABOU:
O FUTURO DA CIBERSEGURANÇA É UM SISTEMA

NO FINAL DE 2025, A CIBERSEGURANÇA ENTROU NUMA NOVA FASE. A EVOLUÇÃO DOS MODELOS DE IA NÃO TROUXE APENAS FERRAMENTAS MAIS CAPAZES; ALTEROU A VELOCIDADE, A ESCALA E O ALCANCE DOS CIBERATAQUES.

Técnicas que antes exigiam equipas altamente especializadas, como criar código de exploração, lançar campanhas credíveis de engenharia social ou encadear ataques complexos, estão hoje mais acessíveis e podem acontecer em minutos.

Ao mesmo tempo, cada agente de IA e cada processo automatizado adotado pelas organizações cria novas identidades, permissões e pontos de exposição. O problema é que muitas estratégias de defesa continuam assentes num modelo desenhado para uma realidade mais lenta: acrescentar uma nova ferramenta sempre que surge uma nova ameaça.


RAJA PATEL, SOPHOS

MAIS FERRAMENTAS NÃO SIGNIFICAM MAIS PROTEÇÃO

Durante décadas, esta lógica pareceu funcionar. Endpoint, e-mail, rede, Cloud, identidade: cada área passou a ter a sua própria solução. Mas mais ferramentas não significam necessariamente mais proteção. Quando a informação fica fragmentada por dezenas de produ-

O CHAMADO “LIMIAR DA POBREZA” EM CIBERSEGURANÇA SURGE QUANDO UMA ORGANIZAÇÃO NÃO CONSEGUE TRANSFORMAR A TECNOLOGIA QUE ADQUIRIU NUMA DEFESA EFICAZ.

tos, a organização responde a ataques coordenados com uma defesa descoordenada. Se o endpoint não partilha o que detetou com a firewall, se a proteção de e-mail não comunica com a identidade e se cada ferramenta decide isoladamente... a defesa chega demasiado tarde.

A Gestão de Informação e Eventos de Segurança (SIEM) e a Deteção e Resposta Ampliadas (XDR) foram passos importantes para reduzir esta fragmentação. A SIEM centralizou registos; o XDR procurou correlacionar deteções entre ferramentas. Continuam a ser capacidades essenciais, mas agregar informação depois de ela ser produzida não é o mesmo que ter uma arquitetura em que todos os pontos de defesa partilham sinais em tempo real e respondem como um só sistema.

Num verdadeiro sistema de defesa, a informação não é apenas recolhida: é partilhada desde o primeiro sinal. Uma deteção num endpoint pode desencadear uma resposta na firewall; uma identidade comprometida pode bloquear acessos em todo o ambiente; um e-mail suspeito pode elevar o nível de alerta nos restantes controlos. Deteção em qualquer ponto, resposta em todo o ambiente.

O FUTURO É UMA DEFESA COORDENADA

A lacuna não é apenas tecnológica. A maioria das organizações não dispõe de um CISO nem de equipas capazes de configurar, monitorizar, validar e melhorar continuamente os controlos de segurança. O chamado “limiar da pobreza” em cibersegurança surge quando uma organização não consegue transformar a tecnologia que adquiriu numa defesa eficaz.

A IA torna esta lacuna ainda mais perigosa, porque os atacantes conseguem adotar novas capacidades rapidamente. No entanto, também pode ajudar a reduzi-la, desde que seja integrada na própria arquitetura de defesa e não adicionada como uma função isolada. A automatização não substitui a supervisão humana; deve permitir detetar e responder mais depressa, enquanto as pessoas definem limites, avaliam riscos e tomam decisões críticas.

É a esta necessidade que responde o Sophos Fusion: uma arquitetura de defesa aberta e nativa de IA que liga endpoints, firewall, e-mail, Cloud, rede, identidade e operações de segurança numa camada comum de dados e inteligência. Ao integrar também ferramentas de terceiros, permite correlacionar sinais, automatizar respostas e beneficiar do conhecimento acumulado perante ameaças detetadas em diferentes ambientes.

Num contexto em que os ataques avançam à velocidade das máquinas, a resposta não passa por acrescentar mais ferramentas, mas por construir um sistema de defesa coordenado, capaz de aprender e atuar em tempo real.



A RECUPERAÇÃO DE RANSOMWARE FALHA ANTES DE CHEGAR AOS DADOS



POR RUI DAMIÃO

OS PLANOS DE RECUPERAÇÃO DE RANSOMWARE SÃO ESCRITOS PARA O CENÁRIO MAIS SIMPLES, ONDE O BACKUP EXISTE, O RTO ESTÁ DEFINIDO E O EXERCÍCIO ANUAL CORRE BEM. NO ENTANTO, NENHUM DESTES PLANOS COSTUMA SOBREVIVER AO PRIMEIRO CONTACTO COM UM ATAQUE REAL. O QUE FALHA NÃO SÃO OS BACKUPS; É O QUE VEM DEPOIS DELES.

A base de tudo o que as organizações pensam saber sobre a sua capacidade de recuperação assenta numa confiança que os estudos não confirmam. Segundo o "*Data Trust and Resilience Report 2026*" da Veeam, que inquiriu mais de 900 responsáveis de IT, segurança e risco a nível mundial, 90% das organizações confiam na sua capacidade de recuperar de um ciberincidente. Menos de um em cada três recuperou efetivamente todos os dados afetados por um ataque de ransomware e 44% recuperou menos de 75%. Com base no estudo, a confiança na recuperação e a prova da recuperação são duas capacidades diferentes.

O desfasamento entre o que as organizações acreditam poder fazer e o que efetivamente conseguem fazer quando o pior acontece separa a preparação teórica da capacidade real de recuperação. Não é apenas uma questão de saber se as empresas têm backups, mas o que quebra depois disso: as dependências, os RTO nunca testados sob pressão real e a infraestrutura de identidade que tem de ser reconstruída antes de qualquer aplicação voltar a funcionar.

O RANSOMWARE JÁ NÃO É UMA QUESTÃO DE MALWARE

Para entender porque é que tantas recuperações falham, é preciso primeiro entender como o ransomware opera hoje, que tem menos a ver com ficheiros maliciosos. Segundo "*Active Adversary Report 2026*" da Sophos, que analisou 661 casos de resposta a incidentes e deteção e resposta geridas, o tempo médio de permanência de um atacante antes de ser detetado desceu para três dias. Dentro dessa janela, a velocidade é o dado mais preocupante, onde, depois de obter acesso inicial, um atacante demora, em média, apenas 3,4 horas a alcançar o servidor de Active Directory.



Marcel Bornhöfft, Associate Field CISO na Sophos, explica que esta aceleração não resulta de novas técnicas, mas da execução mais rápida das que já são conhecidas. "Os atacantes não estão necessariamente a recorrer a um novo manual de ataque; estão a executar o manual já conhecido, mas muito mais depressa", afirma, acrescentando que "o controlo da identidade pode dar a um atacante acesso a contas privilegiadas, sistemas críticos para o negócio e às mesmas ferramentas administrativas utilizadas pela própria equipa de IT da organização". Os números indicam que 67% das causas-raiz identificados nos casos analisados pela Sophos estavam relacionadas com identidade e no "*State of Ransomware 2026*" (onde foram inquiridos 2.158 responsáveis de IT e cibersegurança) 79% dos ataques começaram através de uma abordagem baseada em identidade.

Bruno Castro, Fundador e CEO da VisionWare, descreve o mesmo fenómeno a partir da reconstrução pós-incidente. "A ideia de que o ciberataque só inicia quando os ficheiros foram encriptados é,



MARCEL BORNHÖFFT, SOPHOS

muitas vezes, mal interpretada", sendo que "esse é apenas o momento em que a intrusão se torna visível, tipicamente de forma violenta e ruidosa, para a organização", diz. Bruno Castro nota ainda que este tempo de permanência tem vindo a comprimir-se de forma acentuada ao longo dos anos. "Há 20 anos, estaríamos a falar de meses; hoje, falamos, no máximo, de poucas horas", acrescenta.

Paulo Vieira, Country Manager da Netskope em Portugal, acrescenta a esta descrição a fase que rara-

"O CONTROLO DA IDENTIDADE PODE DAR A UM ATACANTE ACESSO A CONTAS PRIVILEGIADAS, SISTEMAS CRÍTICOS PARA O NEGÓCIO E ÀS MESMAS FERRAMENTAS ADMINISTRATIVAS UTILIZADAS PELA PRÓPRIA EQUIPA DE IT DA ORGANIZAÇÃO"





PAULO VIEIRA, NETSKOPE PORTUGAL

mente é vista antes de a encriptação se tornar visível: a exfiltração de dados. "O ponto cego mais comum é a exfiltração para dupla extorsão: os dados saem antes de qualquer ficheiro ser encriptado, muitas vezes para armazenamento cloud não sancionado (...), usando tráfego TLS que as organizações não inspecionam", explica. Segundo Paulo Vieira, as equipas de segurança "tipicamente têm visibilidade sobre a rede on-prem e talvez sobre os SaaS corporativos oficiais, mas não sobre *uploads* para *tenants* pessoais dessas mesmas aplicações", o que significa que, quando a encriptação se torna finalmente visível, os dados já saíram há muito.

> "O PONTO CEGO MAIS COMUM É A EXFILTRAÇÃO PARA DUPLA EXTORSÃO: OS DADOS SAEM ANTES DE QUALQUER FICHEIRO SER ENCRIPTADO, MUITAS VEZES PARA ARMAZENAMENTO CLOUD NÃO SANCIONADO"

BACKUP COMO PRIMEIRO ALVO, NÃO COMO ÚLTIMO RECURSO

Se há um ponto em que praticamente todos os responsáveis convergem é de que a infraestrutura de backup deixou de ser um sistema secundário para se tornar num dos primeiros alvos de ataque. André Feijóo, Senior Account Executive da Cohesity Portugal, resume a lógica do lado do atacante: "não basta ter os dados protegidos e seguros, é preciso ser rápido a recuperá-los. Quando a arquitetura é antiga e recuperar significa duas ou três semanas de paragem, muitas empresas acabam por pagar mesmo tendo cópias válidas. O atacante sabe disso". Segundo o "*State of Ransomware 2026*", 66% das organizações cujos dados foram encriptados conseguiram recuperar através de backups, um valor que subiu 12 pontos percentuais face ao ano anterior, enquanto o custo médio de recuperação,



"A INFRAESTRUTURA DE BACKUP NÃO É TRATADA COMO UM ATIVO CRÍTICO DE SEGURANÇA E PARTILHA AUTENTICAÇÃO COM A PRODUÇÃO, FICA FORA DOS CICLOS DE ATUALIZAÇÃO E RARAMENTE BENEFICIA DO MESMO NÍVEL DE MONITORIZAÇÃO"



RUI OLIVEIRA, CLARANET PORTUGAL,

excluindo resgates, aumentou 11% para 1,7 milhões de dólares.

Marcel Bornhöfft evita classificar a ideia de atacar backups como uma tática generalizada, sublinhando que "os dados habitualmente citados medem a forma como as organizações recuperam através de backups e não a frequência com que os atacantes tentam comprometer a infraestrutura de cópias de segurança". Ainda assim, reconhece que, "quando os atacantes obtêm acesso privilegiado num ambiente com segmentação insuficiente, as consolas de backup, os *snapshots* e as plataformas de virtualização podem também ficar ao seu alcance".

Rui Oliveira, Security Solutions Specialist na Claranet Portugal, confirma que este cenário já não é uma exceção e que "é um cenário mais frequente do que muitas organizações imaginam" e descreve dois padrões distintos. No primeiro, "a infraestrutura de backup está integrada no mesmo domínio, utiliza as mesmas credenciais administrativas e armazena os dados em recursos acessíveis a partir da rede de produção". No segundo, mais preocupante, "nem é necessária qualquer encriptação", uma vez que "os próprios repositórios são eliminados utilizando funcionalidades legítimas das plataformas". Rui Oliveira acrescenta, ainda, que "a infraestrutura de backup não é tratada como um ativo crítico de segurança e partilha autenticação com a produção, fica fora dos ciclos de atualização e raramente beneficia do mesmo nível de monitorização que os restantes sistemas".



Carlos Caldeira, Cybersecurity Manager e CISO na Oramix, partilha um caso concreto que ilustra esse padrão. Numa organização apoiada recentemente pela empresa, "o sistema de backup partilhava as credenciais de administração do domínio e, assim que essas credenciais foram comprometidas, os atacantes acederam também aos backups pela mesma via, através de movimento lateral". O incidente levou a que a organização perdesse, ao mesmo tempo, "os dados e a única via de recuperação". A equipa teve de reconstruir sistemas manualmente, durante semanas, com um custo muito superior ao que resultaria de um backup segregados da rede de produção.

RTO NUNCA TESTADOS SOB PRESSÃO REAL

O tempo de recuperação objetivo, o número que as organizações comunicam à administração como garantia de resiliência, é, segundo os responsáveis, um dos pontos onde a distância entre teoria e prática mais se sente. Rui Oliveira recorda "um dos casos mais marcantes", com "um RTO de 24 horas formalmente aprovado e comunicado à administração", em que, "ao fim dessas 24 horas, ainda estávamos a preparar a infraestrutura necessária para iniciar a recuperação", tudo porque "não tinha sido considerado o tempo necessário para validar que o ambiente estava efetivamente limpo antes de iniciar as reposições, nem o impacto real dos volumes de dados a transferir face à capacidade disponível de rede e armazenamento".

Carlos Ferreira, Diretor Técnico na Prologin, descreve uma dinâmica semelhante: um cliente "acreditava conseguir recuperar toda a operação crítica em menos de oito horas". O backup funcionava, mas "ninguém tinha considerado o tempo necessário para validar a infraestrutura, reconstruir serviços de identidade, testar aplicações e coordenar equipas de negócio". Assim, diz Carlos Ferreira, "o *recovery* técnico foi relativamente rápido; o *recovery* operacional demorou vários dias".

André Feijóo situa o mesmo problema em escala. "Um RTO de quatro horas medido num servidor é um RTO por servidor, não para 800", nota, explicando que à escala real "o que limita não é o procedimento, é a arquitetura: a capacidade agregada, a rede e o destino da restauração". O representante da Cohesity acrescenta um fator frequentemente esquecido nos exercícios de teste: "num incidente real não se restaura para o ambiente de origem. O ambiente está comprometido, pode estar retido para análise forense por exigência da seguradora e às vezes o próprio hardware é suspeito".

A IDENTIDADE COMO PRÉ-REQUISITO, NÃO COMO MAIS UM SISTEMA A RESTAURAR

Antes de qualquer aplicação de negócio poder ser restaurada, é preciso reconstruir a infraestrutura de identidade e essa reconstrução raramente entra nas contas do RTO original. Carlos Caldeira descreve a sequência que a sua equipa segue.




CARLOS CALDEIRA, ORAMIX

"O ponto de partida é sempre garantir que a infraestrutura de segurança e *networking* não foi comprometida. Só depois disso avançamos com a recuperação de sistemas. Começamos, habitualmente, pelo catálogo de utilizadores, como o Active Directory, e pela infraestrutura de DNS", indica. Sobre o tempo que isso acrescenta, explica que "quando existe imutabilidade validada, falamos de poucas horas. Quando não existe nada disso, o processo pode prolongar-se por vários dias".

> "O SISTEMA DE BACKUP PARTILHAVA AS CREDENCIAIS DE ADMINISTRAÇÃO DO DOMÍNIO E, ASSIM QUE ESSAS CREDENCIAIS FORAM COMPROMETIDAS, OS ATACANTES ACEDERAM TAMBÉM AOS BACKUPS"

Paulo Vieira traz para a equação a camada híbrida que liga a identidade *on-premises* e cloud. "A identidade federada cria uma dependência circular: o SSO para as aplicações SaaS depende muitas vezes do Active Directory on-prem, que pode estar encriptado ou comprometido, o que bloqueia o acesso às próprias ferramentas SaaS necessárias para coordenar a resposta", afirma. Paulo Vieira insiste que restaurar dados é apenas metade do problema, até porque "restaurar cópias de segurança limpas é inútil se a infraestrutura de identidade e os canais de acesso continuarem comprometidos". Assim, a reconstrução da confiança, com "revogação de tokens, rotação de chaves de encriptações e redefinição de permissões" é "frequentemente o verdadeiro gargalo da recuperação".

André Feijóo indica que a maioria das organizações nunca testa este cenário. "A grande maioria das empresas nunca testou uma recuperação total do Active Directory e não tem ferramentas para o fazer de forma automatizada". Quando o processo



é manual, "sob pressão consome facilmente dias ou semanas – só essa fase pode ser mais longa do que o RTO que a empresa comunicou ao negócio".

DEPENDÊNCIAS QUE SÓ A ANÁLISE FORENSE REVELA

Bruno Castro descreve este processo de reconstrução como um exercício de comparar duas versões da mesma organização, onde "a documentação indica, por vezes, que determinados sistemas estão segmentados, que os acessos privilegiados são restritos ou que os backups estão isolados. E, mais tarde, a investigação revela contas com privilégios excessivos, redes de interligação entre ambientes, sistemas aparentemente isolados que continuam a comunicar com componentes críticas". O representante da VisionWare resume que há uma "diferença entre a arquitetura que a organização pensa ter e a arquitetura que o atacante encontrou e acabou por decifrar". Estas dependências, sublinha, "tornam-se evidentes quando reconstruímos o percurso do atacante", nunca antes.



ANDRÉ FEIJÓO, COHESITY PORTUGAL

José Gonçalves, Solution Engineering Manager na Exclusive Networks Portugal, observa o mesmo padrão a partir de uma perspetiva transversal a vários clientes e setores. "As organizações têm backups e planos de Disaster Recovery, mas muitas vezes nunca testaram uma recuperação completa. Quando acontece um ransomware ou outro tipo de ataque grave, descobrem dependências que desconheciam, RTO que não são realistas e falta de clareza sobre o que recuperar primeiro". A conclusão de José Gonçalves aponta para além da tecnologia, onde "o problema

"A GRANDE MAIORIA DAS EMPRESAS NUNCA TESTOU UMA RECUPERAÇÃO TOTAL DO ACTIVE DIRECTORY E NÃO TEM FERRAMENTAS PARA O FAZER DE FORMA AUTOMATIZADAL"



normalmente não é apenas recuperar os dados. É principalmente recuperar os serviços críticos, na ordem certa, dentro do tempo que o negócio consegue suportar".

O QUE SÓ SE RESOLVE ANTES DO INCIDENTE

As políticas de retenção de backups, definidas normalmente para acomodar erros operacionais ou falhas técnicas, raramente foram pensadas para um adversário que já está dentro da rede há dias ou semanas antes de agir. André Feijóo, da Cohesity, identifica que "o padrão típico é uma retenção detalhada de duas a quatro semanas e, para trás disso, apenas cópias mensais com pouca granularidade. Só que o acesso inicial do atacante pode ser muito anterior". Bruno Castro, da VisionWare, propõe uma forma diferente de colocar a questão, que desloca o foco da duração da retenção para a integridade da cópia: "a questão que a forense coloca não é apenas 'quantos dias de backup temos?'. Deve ser, antes, 'temos uma cópia comprovadamente anterior ao compromisso e que o atacante não conseguiu alterar ou eliminar'".

"A DECISÃO É TOMADA COM BASE NO IMPACTO PARA O NEGÓCIO, NÃO NA IMPORTÂNCIA TÉCNICA DOS SISTEMAS. COMEÇAMOS POR IDENTIFICAR QUAIS OS PROCESSOS QUE GERAM RECEITA, SUPORTAM OPERAÇÕES CRÍTICAS OU CUMPREM REQUISITOS LEGAIS"



CARLOS FERREIRA, PROLOGIN

Quando tudo parece crítico, a diferença entre uma recuperação organizada e uma recuperação caótica está numa decisão que devia ter sido tomada muito antes do incidente. Carlos Ferreira, da Prologin, descreve que "a decisão é tomada com base no impacto para o negócio, não na importância técnica dos sistemas. Começamos por identificar quais os processos que geram receita, suportam operações críticas ou cumprem requisitos legais. Depois trabalhamos para trás, restaurando as dependências necessárias".



Importa, também, separar um teste para a *checkbox* com um teste verdadeiro. Carlos Ferreira explica que "um teste de *checkbox* valida apenas se os dados podem ser restaurados. Um teste eficaz valida se as organizações conseguem voltar a operar". O representante da Prologin acrescenta que "se o teste não gerar desconforto nem descobrir problemas, provavelmente não foi suficientemente realista".

O EFEITO NIS2

Com a NIS2 em vigor, a pergunta que os fornecedores ouvem dos clientes portugueses mudou, mas nem toda a gente mudou ao mesmo ritmo. José Gonçalves descreve que, "antes, a principal preocupação era garantir que existiam backups. Hoje, a pergunta é cada vez mais 'se acontecer alguma coisa, conseguimos mesmo recuperar?'". Rui Oliveira, da Claranet Portugal, confirma esta divisão em dois grupos. Nas organizações "onde existe envolvimento da administração, a NIS2 tem servido como catalisador para iniciativas concretas", com pedidos de "exercícios de recuperação completos, testes de crise e validação de RTO". No entanto, persiste "um conjunto significativo de organizações cuja principal preocupação é a componente documental e de conformidade", ou seja, planos e políticas atualizados, "mas pouca evidência de que a capacidade de recuperação tenha sido efetivamente testada".



BRUNO CASTRO, VISIONWARE

Carlos Caldeira situa a mudança no tipo de prova que passou a ser exigida. "Mostrar que existem políticas e procedimentos sem demonstrar a sua aplicabilidade e evidências é, no mínimo, redutor". Segundo

> "A DOCUMENTAÇÃO INDICA, POR VEZES, QUE DETERMINADOS SISTEMAS ESTÃO SEGMENTADOS, QUE OS ACESSOS PRIVILEGIADOS SÃO RESTRITOS OU QUE OS BACKUPS ESTÃO ISOLADOS. E, MAIS TARDE, A INVESTIGAÇÃO REVELA CONTAS COM PRIVILÉGIOS EXCESSIVOS"




JOSÉ GONÇALVES, EXCLUSIVE NETWORKS PORTUGAL

"QUANDO ACONTECE UM RANSOMWARE OU OUTRO TIPO DE ATAQUE GRAVE, [AS ORGANIZAÇÕES] DESCOBREM DEPENDÊNCIAS QUE DESCONHECIAM, RTO QUE NÃO SÃO REALISTAS E FALTA DE CLAREZA SOBRE O QUE RECUPERAR PRIMEIRO"

o representante da Oramix, a NIS2 "impulsionou a que a resiliência não se demonstre apenas com documentação e sim através da capacidade comprovada de recuperar serviços críticos quando o pior cenário acontece".

José Gonçalves acrescenta um dado que confirma o efeito prático desta pressão regulatória, onde, nas organizações que já sofreram um incidente grave, se observa uma "mudança clara de maturidade" e deixam de olhar apenas para a existência de backups e "começam a preocupar-se muito mais com a capacidade efetiva e a rapidez de recuperação". No fundo, "passam de uma abordagem teórica de recuperação para uma abordagem operacional, testada e orientada à continuidade do negócio".

É precisamente essa passagem de plano documentado para capacidade demonstrada que separa as organizações que sobrevivem a um ransomware das que apenas acreditavam estar preparadas. Os dados do "*IT Resilience Survey 2026: Ransomware Recovery and Readiness*" da Gartner confirmam que a maioria das organizações já implementou as ferramentas fundamentais: cerca de 70% utiliza software de backup com automação e 78% implementou, ou está a implementar, ambientes de recuperação isolados. Mas o mesmo estudo conclui que, apesar destes investimentos, muitas organizações continuam a não conseguir utilizar eficazmente essas capacidades quando mais precisam delas, normalmente por falta de estratégia integrada e de coordenação entre o IT e o negócio. É este o *gap* que a Veeam mediu em 90% contra 28%. A tecnologia, na maioria dos casos, já está presente. O que falta continua a ser aquilo que o *checkbox* não consegue certificar: a prova, sob pressão real, de que tudo funciona em conjunto.

COHESITY

"A MÉTRICA MUDOU: JÁ NÃO BASTA TER BACKUP, É PRECISO SABER QUANTO TEMPO DEMORA A RECUPERAR"


ANDRÉ FEIJÓO, SENIOR ACCOUNT EXECUTIVE, DA COHESITY

A CIBER-RESILIÊNCIA DEIXOU DE SER APENAS UMA PREOCUPAÇÃO DAS EQUIPAS DE INFRAESTRUTURA PARA ASSUMIR UM PAPEL CENTRAL NA ESTRATÉGIA DE CIBERSEGURANÇA E DE CONTINUIDADE DO NEGÓCIO. EM ENTREVISTA À IT SECURITY, ANDRÉ FEIJÓO, SENIOR ACCOUNT EXECUTIVE, DA COHESITY, EXPLICA POR QUE RAZÃO AS ORGANIZAÇÕES DEVEM PREPARAR-SE PARA RECUPERAR NUM CENÁRIO REAL DE CIBERATAQUE, COM DADOS PROTEGIDOS, AMBIENTES LIMPOS E PRIORIDADES BEM DEFINIDAS, E DEFENDE QUE O VERDADEIRO TESTE JÁ NÃO É SABER SE O BACKUP FOI FEITO, MAS QUANTO TEMPO É NECESSÁRIO PARA VOLTAR A OPERAR.

Porque é que a ciber-resiliência se tornou numa prioridade crítica na agenda das organizações portuguesas nos últimos anos?

Os ciberataques deixaram de ser um risco teórico e passaram a parar operações. Prevenir não é suficiente. O Banco Central Europeu define ciber-resiliência como proteger dados e sistemas de ciberataques e, em caso de ataque bem-sucedido, retomar rapidamente a operação. É a segunda parte que faltava. Isso mudou os interlocutores. A plataforma de backup continua a ser da infraestrutura, mas tem de fazer parte da estratégia de cibersegurança, por isso falar com as equipas de segurança é indispensável. E passámos a falar com quem responde pelo negócio,

"OS CIBERATAQUES DEIXARAM DE SER UM RISCO TEÓRICO E PASSARAM A PARAR OPERAÇÕES. PREVENIR NÃO É SUFICIENTE. O BANCO CENTRAL EUROPEU DEFINE CIBER-RESILIÊNCIA COMO PROTEGER DADOS E SISTEMAS DE CIBERATAQUES E, EM CASO DE ATAQUE BEM-SUCEDIDO, RETOMAR RAPIDAMENTE A OPERAÇÃO".

onde a pergunta já não é "está o backup feito" mas "quanto tempo demoramos a recuperar".

O que significa, na prática, uma estratégia de proteção de dados a 360 graus e que elementos deve incluir para além do backup?

É responder a uma sequência: que dados tenho, onde estão, quais são críticos, estão limpos e em que ordem os levanto. O backup responde a uma. As outras exigem classificação, cópias imutáveis e isoladas e deteção de malware antes do restauro. E a identidade: sem Active Directory ou Entra ID recuperado, não há aplicações para levantar. Muitas ainda não sabem quanto tempo demoram a recuperar todo o seu Active Directory.

Como está a evoluir o conceito de backup tradicional para uma abordagem de resiliência e que fatores estão a acelerar essa mudança?

O backup tradicional foi feito para acidentes: assumia um ambiente saudável para onde voltar. O ransomware acabou com isso: entra, estuda o ambiente e ataca primeiro o backup. Muitas empresas com que falo continuam nesse modelo. E recuperar sem eliminar a ameaça leva muitas vezes a reinfeção. A métrica mudou: não interessa se o job correu de noite, interessa quanto demora a retomar a operação.

Que boas práticas recomenda às organizações para minimizar interrupções do negócio e acelerar a recuperação após um incidente?

Primeiro, definir o que na Cohesity chamamos minimum viable company: os serviços que têm de estar de pé nas primeiras horas e de que dependem. Depois, cópias imutáveis e isoladas, com credenciais separadas da produção, recuperar para ambiente limpo e validar integridade. E ensaiar recuperações em cenário de ciberataque: o que se faz primeiro, quem se contacta, que sistemas se levantam e em que ordem, começando pela identidade.

Quais são os principais desafios de cibersegurança que as organizações portuguesas enfrentam atualmente?

Nestes dois anos em Portugal, o que mais noto são equipas pequenas com demasiadas ferramentas e a falta de testes reais de recuperação em cenário de

"AJUDAMOS AS MAIORES EMPRESAS DO MUNDO A FAZER EXATAMENTE ISSO. MAIS DE 12.000 ORGANIZAÇÕES CONFIAM-NOS OS SEUS DADOS, ENTRE ELAS MAIS DE 85 DAS FORTUNE 100, E ISSO DÁ-NOS UMA LEITURA CLARA DO QUE FUNCIONA E DO QUE FALHA QUANDO É PRECISO RECUPERAR A SÉRIO".

ciberataque. Quase ninguém testou uma recuperação massiva nem tem clean room. E a regulação passou a pedir prova: demonstrar que se sabe recuperar, não que há backups.

Como se podem as organizações preparar melhor para a evolução constante das ciberameaças e que papel pode a Cohesity desempenhar nessa preparação?

Preparar-se é assumir que o ataque vai acontecer e treinar a recuperação: saber o que é crítico, ter cópias que o atacante não consiga apagar, levantar os sistemas em ambiente isolado e medir quanto demora. Automatizar, para reduzir passos manuais e ganhar tempo.

Ajudamos as maiores empresas do mundo a fazer exatamente isso. Mais de 12.000 organizações confiam-nos os seus dados, entre elas mais de 85 das Fortune 100, e isso dá-nos uma leitura clara do que funciona e do que falha quando é preciso recuperar a sério. A ciber-resiliência é o nosso foco e é aí que investimos, com a IA a fazer parte disso: deteta comportamentos anómalos nos dados antes de o problema crescer, acelera a recuperação com menos trabalho manual e transforma os dados protegidos numa base de conhecimento. Em vez de um arquivo que ninguém consulta, o backup passa a responder a perguntas em linguagem natural, com respostas ancoradas nos documentos da própria empresa, sem tocar nos sistemas de produção.

Como se podem as organizações preparar melhor para a evolução constante das ciberameaças e que papel pode a Cohesity desempenhar nessa preparação?

Preparar-se é assumir que o ataque vai acontecer e treinar a recuperação: saber o que é crítico, ter cópias que o atacante não consiga apagar, levantar os sistemas em ambiente isolado e medir quanto demora. Automatizar, para reduzir passos manuais e ganhar tempo.

Ajudamos as maiores empresas do mundo a fazer exatamente isso. Dois terços das empresas da Global 500 confiam na Cohesity para fornecer segurança de dados com IA. Isso dá-nos uma leitura clara do que funciona e do que falha quando é preciso recuperar a sério. A ciber-resiliência é o nosso foco e é aí que investimos, com a IA a fazer parte disso: deteta comportamentos anómalos nos dados antes de o problema crescer, acelera a recuperação com menos trabalho manual e transforma os dados protegidos numa base de conhecimento. Em vez de um arquivo que ninguém consulta, o backup passa a responder a perguntas em linguagem natural, com respostas ancoradas nos documentos da própria empresa, sem tocar nos sistemas de produção. ◀

por Carlos Caldeira,
Cybersecurity Manager e CISO, Oramix

NINGUÉM TESTA A RECUPERAÇÃO ATÉ PRECISAR DELA

IMUTABILIDADE, DETEÇÃO, REMEDIAÇÃO E RESPOSTA ESPECIALIZADA RARAMENTE SÃO TESTADAS EM CONJUNTO, ATÉ UM INCIDENTE OBRIGAR A ISSO.

Enquanto CISO, defendo há anos que a resiliência digital assenta em quatro pilares: imutabilidade de dados, deteção e resposta avançada através de XDR, capacidades de remediação e rollback, e serviços especializados de resposta a incidentes (CSIRT as a Service). As ameaças atuais já não se limitam à indisponibilidade dos sistemas: impactam dados, operações e a confiança de clientes e parceiros. Um estudo da Omdia*, de junho de 2026, mostra que 83% das organizações sofreram um ataque de ransomware bem-sucedido nos últimos 24 meses, e menos de quatro em cada dez recuperaram a maior parte dos dados depois do ataque. O que separa estes dois grupos raramente é a tecnologia. É se, algum dia, testaram os quatro pilares em conjunto. Recentemente, apoiámos uma organização que só descobriu a resposta durante o próprio incidente.

IMUTABILIDADE DE DADOS

Um backup verdadeiramente imutável não pode ser apagado, nem por um administrador com acesso total, nem por um atacante que lhe roube as credenciais. É essa separação de privilégios que o transforma na última linha de defesa. Nesta organização, a solução de backup estava integrada no Active Directory,


CARLOS CALDEIRA, ORAMIX

partilhando a cadeia de autenticação que sustentava o resto do ambiente. Não havia imutabilidade real; quando as credenciais de administração foram comprometidas, os atacantes eliminaram também os backups, e com eles, a única via de recuperação sem reconstrução total.

DETEÇÃO E RESPOSTA AVANÇADA ATRAVÉS DE XDR

Uma plataforma XDR combina políticas definidas com aprendizagem contínua, através de IA, sobre o comportamento real do ambiente. É essa combinação que permite identificar, numa fase precoce, um movimento lateral antes que se torne um incidente maior. Nesta organização, essa visibilidade não existia: os atacantes permaneceram dentro da infraestrutura durante um período prolongado sem serem identificados.

CAPACIDADES DE REMEDIAÇÃO E ROLLBACK

Para remediar um incidente é necessário isolar o equipamento comprometido, eliminar artefactos maliciosos e bloquear contas afetadas antes que o ataque se propague, mantendo a custódia da prova. Já o rollback permite reverter os sistemas atingidos para o último estado operacional seguro. As duas capacidades reduzem drasticamente o tempo de recuperação, mas só se existir um estado seguro para onde reverter. Nesta organização, sem mecanismos de contenção nem um backup limpo, não havia isolamento possível nem estado seguro a que voltar. O incidente alastrou-se antes de a recuperação sequer poder começar.

CSIRT AS A SERVICE

Mesmo com deteção e remediação a funcionar, a decisão sobre o que conter, isolar, investigar e comunicar durante um incidente real exige competências que a maioria das equipas internas nunca desenvolveu. Foi essa capacidade que também faltou a esta organização: sem uma equipa especializada de CSIRT as a Service, a resposta ficou entregue a quem nunca tinha gerido um incidente desta escala. A recuperação prolongou-se por semanas, entre reconstrução de sistemas e recuperação manual de informação, com forte impacto operacional e financeiro.

RESILIÊNCIA MEDE-SE NA RECUPERAÇÃO, NÃO NA PREVENÇÃO

Este caso não é excecional: é o que acontece quando os quatro pilares nunca foram testados em conjunto e a resposta a um incidente fica entregue a quem não tem experiência real num cenário de crise. Nas avaliações de maturidade que a Oramix realiza, a falha mais comum nunca está numa destas tecnologias isoladamente. Está no momento em que têm de funcionar juntas, sob pressão. E é aí que se decide se uma organização volta à operação em dias, ou continua, semanas depois, a explicar a clientes e parceiros porquê, com o custo que isso tem. Na maioria das organizações, é ainda a área de segurança que tem de insistir nesse teste junto da gestão de topo, antes que seja um incidente a fazê-lo.

** Estudo da Omdia, "Recovery Without Compromise: The Data-Backed Case for Backup Storage with Absolute Immutability", junho de 2026.*

VisionWare since 2005

por Bruno Castro,
Fundador & CEO da VisionWare. Especialista em Cibersegurança e Análise Forense

RANSOMWARE E A DIFERENÇA ENTRE RESTAURAR E RECUPERAR

O RANSOMWARE COMEÇA A PARECER-SE MAIS COM A VELHA ECONOMIA DO CRIME ORGANIZADO DO QUE COM AQUILO QUE TRADICIONALMENTE ASSOCIÁVAMOS A UM CIBERATAQUE. HÁ GRUPOS ESPECIALIZADOS EM OBTER ACESSO INICIAL, OUTROS QUE SE DEDICAM À EXTORSÃO, OPERADORES DE RANSOMWARE-AS-A-SERVICE, INTERMEDIÁRIOS, NEGOCIADORES E MERCADOS ONDE SE COMPRAM E VENDEM ACESSOS A ORGANIZAÇÕES COMPROMETIDAS.

Mas há uma diferença importante face ao modelo de crime organizado que conhecemos, é que neste caso tudo é cada vez mais automatizado. O ransomware-as-a-service permite que ferramentas, infraestruturas e processos de ataque sejam disponibilizados a diferentes operadores, reduzindo a necessidade de conhecimento técnico e tornando possível executar ataques em escala e com muito menos intervenção humana.

O resultado é um modelo de negócio que não só se profissionalizou, como ganhou velocidade. Tal impacta também o tempo "oculto" de permanência na rede. Hoje, o intervalo entre a intrusão, roubo ou até encriptação/destruição, é cada vez mais rápido, passando de meses, semanas, e dias para apenas poucas horas.

O atacante já não precisa necessariamente de permanecer durante muito tempo para causar impacto se tiver acesso às ferramentas certas e encontrar uma


BRUNO CASTRO, VISIONWARE

PERCEBER QUEM NOS PODE ATACAR, QUE MODELO ECONÓMICO ESTÁ POR TRÁS DESSE GRUPO, QUE TIPO DE INFORMAÇÃO OU OPERAÇÃO TEM VALOR PARA ELE, QUANTO TEMPO PODERÁ PERMANECER INVISÍVEL E QUAIS SÃO OS MOMENTOS EM QUE A NOSSA ORGANIZAÇÃO FICARIA MAIS VULNERÁVEL À PRESSÃO.

organização pouco preparada para detetar e reagir, pode passar rapidamente da intrusão à extorsão.

É por isso que a capacidade de detetar e reagir ganha uma importância que vai muito além da monitorização de alertas. Quando o tempo disponível para perceber o que está a acontecer e conter o ataque é cada vez menor, não basta saber que um incidente ocorreu. É preciso conseguir identificar sinais relevantes, perceber rapidamente o que está comprometido, isolar sistemas, proteger identidades e tomar decisões enquanto o ataque ainda está a decorrer – é aqui que entra a recuperação.

Um dos maiores erros é confundir um restore bem-sucedido com recuperação. Restaurar uma máquina virtual prova que sabemos restaurar uma máquina virtual. Não prova que conseguimos recuperar uma empresa.

Também aqui o tempo de permanência do atacante é outra questão a ter em conta nesta equação. Se esteve dentro da organização durante semanas ou meses, uma retenção de 30 ou 60 dias pode não garantir a existência de uma cópia em que ainda possamos confiar. Ter muitos backups não significa necessariamente ter um bom ponto de recuperação. E, quando o tempo entre a intrusão e a destruição dos sistemas diminui, saber onde está a última cópia íntegra torna-se ainda mais importante.

Isto muda a discussão sobre recuperação e obriga a repensar os exercícios de segurança. Talvez seja necessário dar menos atenção ao número de backups, ainda que continue a ser importante, e mais atenção à capacidade real de reconstrução. Devemos testar a recuperação da identidade, validar os backups fora do ambiente comprometido, mapear as dependências das aplicações críticas e medir os tempos reais de recuperação.

Mais importante ainda: estes processos não podem existir apenas num documento. Têm de estar estudados, documentados e testados. É num exercício de recuperação, e não numa apresentação, que se percebe se uma organização sabe realmente o que fazer quando deixa de poder confiar nos seus sistemas.

Além disso, se o ransomware se tornou suficientemente profissional para estudar o nosso negócio antes de o atacar, talvez esteja na altura de nós fazermos o mesmo com o ransomware. Perceber quem nos pode atacar, que modelo económico está por trás desse grupo, que tipo de informação ou operação tem valor para ele, quanto tempo poderá permanecer invisível e quais são os momentos em que a nossa organização ficaria mais vulnerável à pressão.

Se amanhã deixássemos de poder confiar em tudo o que está dentro da nossa rede, o que conseguiríamos reconstruir e quanto tempo demoraria? Se não soubermos responder, não temos necessariamente um problema de backups. Temos sim, um problema de resiliência. ◀

POR RUI DAMIÃO

QUANTUM-SAFE: TER SUPORTE PARA A TECNOLOGIA NÃO SIGNIFICA ESTAR PROTEGIDO POR ELA

A UNIÃO EUROPEIA JÁ FIXOU O FINAL DE 2026 COMO O PRAZO PARA OS ESTADOS-MEMBROS INICIAREM A TRANSIÇÃO PARA A CRIPTOGRAFIA RESISTENTE A COMPUTADORES QUÂNTICOS. EM PORTUGAL, NÃO É POSSÍVEL INDICAR QUANTAS ORGANIZAÇÕES JÁ FIZERAM SEQUER O INVENTÁRIO CRIPTOGRÁFICO QUE ESSE PROCESSO EXIGE. O PROBLEMA, NO ENTANTO, DEIXOU DE SER TÉCNICO E PASSOU A SER DE GESTÃO.

Desde junho de 2025, quando a União Europeia adotou o "*Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography*", que existe uma data concreta sobre os departamentos de segurança: os Estados-membros devem iniciar a transição para a criptografia pós-quântica (PQC) até final de 2026, com os casos de risco elevado protegidos até 2030. O prazo deixou de ser apenas uma referência distante para se tornar num marco a pouco meses de distância.

Os números do mercado confirmam a mudança de tom. A Gartner descreve, no seu relatório de tendências para 2026, a computação quântica não como um horizonte de planeamento a dez anos, mas como um prazo de ação fixado em 2030. A Forrester estima que os gastos com segurança quântica vão ultrapassar os 5% do orçamento total de segurança de IT em 2026, um sinal de que o tema passou de investigação a aprovisionamento. Ainda assim, o inquérito "*Quantum Readiness Outlook*" da Digicert, de julho de 2026, mostra que 87% das organizações dizem estar a planear, testar ou implementar PQC, mas só 7% tem mais de metade dos certificados digitais já em criptografia *quantum-safe* ou híbrida, uma distância grande entre a intenção e a execução.

"Não dispomos de uma métrica consolidada para Portugal", afirmam Henrique Silva e Tiago Andrade, Senior Client Executives da NetApp. "A nossa perceção é que apenas uma minoria concluiu um inventário abrangente das dependências criptográficas, estando a maioria ainda nas fases de descoberta, avaliação e planeamento".

O INVENTÁRIO QUE AINDA NÃO EXISTE

A ausência de dados consolidados não é exclusiva de Portugal. Um inquérito conjunto da BSI alemã com a KPMG encontrou uma realidade semelhante, com menos de 5% das organizações alemãs a terem hoje um plano formal de migração.

Michael Osborne, CTO da IBM Quantum Safe, prefere não tratar esta fase como uma questão de erros. "A transição para a criptografia pós-quântica não deve ser encarada como uma questão de 'erros' por parte das organizações", defende. O problema está antes na forma como a criptografia foi historicamente implementada. "Ao longo de décadas, a criptografia foi sendo integrada de forma estática e, muitas vezes, sem documentação em aplicações legadas, código de terceiros, equipamentos de rede e tecnologias operacionais", explica.

Para Henrique Silva e Tiago Andrade, o erro mais comum não é a inação, mas o âmbito limitado da análise e limitar essa análise às aplicações mais visíveis. "Muitas dependências criptográficas estão incorporadas em sistemas legados certificados, mecanismos de autenticação, gestão de chaves, dispositivos e integrações de terceiros". A IDC prevê que 40% das organizações do Global 2000 vão contratar serviços externos de avaliação de risco quântico até 2027.

Perante um inventário incompleto, a pergunta seguinte é estratégica: substituir algoritmos diretamente ou investir numa arquitetura de *crypto-agility*, capaz de trocar mecanismos criptográficos sem reformular sistemas inteiros. Os representantes da NetApp indicam que a resposta depende do contex-


MICHAEL OSBORNE, IBM QUANTUM SAFE

to. “A substituição direta pode ser suficiente em sistemas simples e isolados”, explicam, acrescentando que, em “ambientes complexos, com dados de longa duração, múltiplas integrações e requisitos regulatórios, exigem *crypto-agility*”.

Michael Osborne recusa a dicotomia e explica que, “em ambientes empresariais”, a substituição direta de algoritmos e a *crypto-agility* “não são abordagens mutuamente exclusivas”, até porque “a *crypto-agility* é um requisito fundamental para garantir a resiliência a longo prazo”.

O denominador comum entre as duas abordagens, segundo os representantes do IBM Quantum Safe e da NetApp, é mapear antecipadamente onde a criptografia está a ser usada. Sem esse mapa, nenhuma das duas decisões tem um ponto de partida.

"AO LONGO DE DÉCADAS, A CRIPTOGRAFIA FOI SENDO INTEGRADA DE FORMA ESTÁTICA E, MUITAS VEZES, SEM DOCUMENTAÇÃO EM APLICAÇÕES LEGADAS, CÓDIGO DE TERCEIROS, EQUIPAMENTOS DE REDE E TECNOLOGIAS OPERACIONAIS"

O QUE JÁ ESTÁ A SER COPIADO

O risco de ‘*harvest now, decrypt later*’, ou seja, a recolha de dados cifrados hoje para serem decifrados assim que existir um computador quântico com relevância criptográfica, é o argumento mais citado para justificar a urgência, mesmo sem data certa para essa capacidade existir.

Para Henrique Silva e Tiago Andrade, a prioridade deve seguir o valor e a duração da informação, ou seja, “devem ser priorizados os dados mais sensíveis e com maior vida útil: propriedade intelectual, dados clínicos, informação financeira estratégica, dados pessoais sensíveis, segredos comerciais e informação sujeita a retenção prolongada”.

Michael Osborne partilha o diagnóstico e acrescenta um dado temporal: o risco não é hipotético. “As organizações devem também ter em conta que os ataques to tipo ‘*harvest now, decrypt later*’ já são uma realidade”, afirma. “Quanto mais cedo iniciarem a sua jornada rumo à adoção de soluções *quan-*


HENRIQUE SILVA, NETAPP


TIAGO ANDRADE, NETAPP

tum-safe, melhor preparadas estarão para mitigar esse risco".

Bruno Gonçalves, Cybersecurity & Public Safety Business Unit Manager da Warpcom, aponta um equívoco que observa junto de clientes portugueses: o de assumir que atualizar infraestrutura resolve automaticamente o problema. "Ter suporte para uma tecnologia não significa estar protegido por ela", resume. Uma aplicação pode passar a suportar algoritmos pós-quânticos e continuar, na prática, a usar os mecanismos antigos, porque a nova funcionalidade nunca chegou a ser ativada.

O MAIOR OBSTÁCULO

À medida que cresce a oferta de soluções *quantum-safe*, cresce também o número de mecanismos proprietários que reivindicam proteção equivalente às normais oficiais. Michael Osborne aponta que "as normas publicadas pelo NIS, como a FIPS 203 (ML-KEM), a FIPS 204 (ML-DAS) e a FIPS 205 (SLH-DAS), são o resultado de quase uma década de rigoroso escrutínio internacional". As alternativas proprietárias, acrescenta, "não beneficiam do mesmo nível de análise pública formal, nem da mesma interoperabilidade alargada no ecossistema tecnológico".

"MUITAS DEPENDÊNCIAS CRIPTOGRÁFICAS ESTÃO INCORPORADAS EM SISTEMAS LEGADOS CERTIFICADOS, MECANISMOS DE AUTENTICAÇÃO, GESTÃO DE CHAVES, DISPOSITIVOS E INTEGRAÇÕES DE TERCEIROS".

HENRIQUE SILVA E TIAGO ANDRADE, SENIOR CLIENT EXECUTIVES DA NETAPP



A posição da NetApp segue uma direção semelhante e Henrique Silva e Tiago Andrade explicam que "a designação quantum-safe não substitui a normalização e a validação independente". Isso não significa, sublinham, que uma solução proprietária seja insegura, apenas que essa equivalência tem de ser demonstrada e não presumida.

O peso desta discussão extravasa os fornecedores de segurança. A Google fixou março de 2026 como o momento de definir 2029 como prazo de migração completa para PQC em toda a sua infraestrutura, alinhando-se com o compromisso já assumido pela Cloudflare. A questão que persiste é quanto dessa proteção cobre sistemas fora do *hyperscaler*, como identidade, assinatura de código, VPN, *legacy* e *on-premises*, onde, segundo as três empresas contactadas, a exposição real se concentra.

Questionados sobre o principal entrave à migração, a IBM e a NetApp explicam que a dificuldade central já não é a viabilidade dos algoritmos, mas a complexidade acumulada em décadas de infraestrutura híbrida. "O principal desafio para a maioria das organizações é gerir a enorme complexidade dos ambientes híbridos de IT", diz Michael Osborne, notando que a sensibilização das lideranças aumentou "graças à atenção regulatória da União Europeia", mas transformar isso em ação exige "ferramentas eficazes de descoberta e uma clara atribuição de responsabilidades".

Henrique Silva e Tiago Andrade descrevem um obstáculo semelhante, com uma nuance sobre perceção de risco. "O principal obstáculo é a combinação entre complexidade dos sistemas legados e uma perceção insuficiente de urgência. Muitas organizações reconhecem o risco, mas ainda não o converteram num programa estruturado, com responsabilidades, prioridades e orçamento", referem.

Bruno Gonçalves acrescenta uma leitura sobre a distribuição setorial dessa maturidade em Portugal. "A banca e a defesa são os setores onde sentimos maior sensibilização para este tema", nota o responsável da Warpcom, atribuindo a diferença à natureza da informação protegida e à existência de equipas especializadas. Já a saúde, a energia e as *utilities*, diz, "já deveriam estar a dar maior prioridade a este risco", pela sensibilidade da informação clínica e pela criticidade e longos ciclos de vida dos sistemas nesses setores.

POR ONDE COMEÇAR COM O ORÇAMENTO QUE HÁ

Quando confrontados com a pergunta mais prática – por onde deve um CISO português começar com o orçamento de que dispõe –, as respostas da IBM convergem quase ponto por ponto. "Pelo inventário criptográfico", respondem Henrique Silva e Tiago Andrade. "É essencial identificar onde estão utilizados algoritmos, certificados e chaves, quais os dependentes e que dados necessitam de permanecer confidenciais durante mais tempo. Sem esse mapa, não é possível definir prioridades nem orçamentar a transição", explicam.

Michael Osborne propõe uma sequência em três etapas: "criar visibilidade", com um inventário e um Cryptographic Bill of Materials; "alinhar as equipas", definindo responsabilidades entre tecnologia, negócio e aprovisionamento; e só depois "executar a mudança com arquiteturas de *crypto-agility* integradas na modernização tecnológica".

Sobre o impacto no desempenho, a IBM desvaloriza a capacidade de processamento como fator crítico. Michael Osborne nota que "as principais considerações operacionais não estão relacionadas com a capacidade de processamento em si, mas sobretudo com os tamanhos das chaves e das assinaturas digitais". A NetApp remete a resposta para o terreno: o impacto "varia significativamente consoante o algoritmo, o protocolo, a arquitetura e o caso de utilização", dizem Henrique Silva e Tiago Andrade,


BRUNO GONÇALVES, WARPCOM

devendo ser medido "através de testes controlados e provas de conceito".

O prazo de dezembro de 2026 pede às organizações portuguesas que esse mapeamento esteja iniciado, com os responsáveis nomeados e um plano aprovado, não que a migração esteja concluída. É uma fasquia mais baixa do que a ideia de resolver a criptografia pós-quântica de uma vez, mas é também a primeira em que adiar deixa de ser uma opção silenciosa, e passa a ser uma decisão que terá de ser justificada perante reguladores, clientes e seguradoras.◀

"A BANCA E A DEFESA SÃO OS SETORES ONDE SENTIMOS MAIOR SENSIBILIZAÇÃO PARA ESTE TEMA"

claranet®

por David Grave,
Cyber Security Senior Director,
Claranet Portugal

ATÉ QUANDO ESTARÃO SEGUROS OS DADOS QUE CIFRAMOS HOJE?

SE NÃO SABEMOS POR ONDE OS DADOS PASSAM NEM DURANTE QUANTO TEMPO PRECISAM DE PERMANECER CONFIDENCIAIS, PODEMOS ESTAR A PROTEGER HOJE AQUILO QUE ALGUÉM CONSEGUIRÁ LER AMANHÃ.

No dia 6 de junho de 2019, uma empresa europeia de infraestrutura digital anunciou inadvertidamente a um grande operador internacional, através de um ponto de interligação em Frankfurt, mais de 70.000 rotas que não lhe pertenciam. Durante mais de duas horas, uma parte significativa do tráfego destinado a redes móveis europeias foi encaminhada através da rede desse operador antes de seguir para o destino legítimo.

Não houve uma falha generalizada, um ataque de *ransomware* ou um alerta no SOC. Para o utilizador, o incidente traduziu-se apenas numa aplicação mais lenta, numa videochamada a perder qualidade ou numa sessão de VPN a restabelecer a ligação. O CERT-EU documentou o incidente e sublinhou que os desvios de BGP desta natureza costumam durar apenas alguns minutos.

O caso torna visível aquilo que habitualmente fica escondido: uma alteração de caminho pode acontecer em grande escala, durar horas e deixar a maioria dos utilizadores apenas com a sensação de que a rede está estranha.

Mas a mesma fragilidade que permite um desvio acidental pode também ser explorada deliberadamente. A questão deixa então de ser apenas "por que razão o tráfego foi desviado?" e passa a ser outra: "o que acontece quando continua a chegar ao destino, mas por um caminho que nunca escolhemos?". A primeira pergunta é de engenharia de redes. A segunda é já de *cibersegurança* e de *threat intelligence*.



O encaminhamento entre operadores continua a assentar num modelo de confiança distribuída. Um sistema autónomo anuncia que alcança determinado prefixo e as redes vizinhas aceitam e propagam esse anúncio de acordo com as suas políticas. Como o protocolo não foi originalmente concebido com mecanismos robustos de autenticação e validação, um anúncio incorreto ou malicioso pode alterar o percurso do tráfego sem interromper a sua entrega. Para o utilizador, o serviço continua operacional; para a organização, o destino continua a responder; para o *SOC*, pode não existir qualquer indicador clássico de compromisso. No entanto, durante esse intervalo, o tráfego pode atravessar uma infraestrutura que não fazia parte do caminho previsto.

Perante este cenário, a cifragem do tráfego pode parecer suficiente para eliminar o risco de interceção. Contudo, embora um atacante que intercete tráfego TLS corretamente implementado não consiga ler o conteúdo, pode observar padrões de comunicação, pontos terminais, horários, volumes e comportamentos – metadados valiosos para quem os sabe analisar. Segundo uma investigação recente das universidades de Princeton e da Virgínia, estes ataques permitem *monitorização*, *fingerprinting*, manipulação e descarte de tráfego, tudo isto sem quebrar a cifra.

O risco, porém, não termina no momento da interceção. Mesmo que o conteúdo permaneça ilegível hoje, o tráfego cifrado pode ser armazenado para ser decifrado no futuro, quando a computação quântica tiver capacidade para comprometer os algoritmos atualmente utilizados. É esta ameaça, conhecida como "*store now, decrypt later*", que torna urgente a transição para a criptografia pós-quântica.

Neste contexto, a União Europeia publicou um roteiro coordenado que prevê o início desta transição até ao final de 2026 e a proteção dos casos de utilização de risco elevado até 2030. Também o NIST definiu um calendário para a descontinuação dos algoritmos clássicos com um nível de segurança de 112 bits depois de 2030 e a sua proibição depois de 2035.

Emerge assim uma nova ameaça. Hoje, alguém pode copiar tráfego cifrado. Amanhã, pode existir capacidade para atacar a criptografia que o protege. Isto não significa que todas as alterações de encaminhamento sejam operações de espionagem. Significa que temos de conseguir distinguir um erro operacional de uma interceção deliberada. Caso contrário, estaremos a tratar um problema de deteção de ameaças como se fosse apenas um problema de operações de rede.

Durante anos, concentrámos a *segurança* no destino e na identidade, com EDR, XDR, SIEM, SOC e Zero Trust. Tudo isto é necessário, mas proteger a informação exige também compreender e monitorizar o caminho que percorre. Se esse caminho mudar, a comunicação pode continuar a chegar ao destino, o utilizador permanecer autenticado e a aplicação disponível, mesmo que o tráfego atravesse uma infraestrutura que não fazia parte da equação.

A criptografia pós-quântica pode ser essencial para garantir que aquilo que protegemos hoje continua seguro amanhã. Mas trocar algoritmos não basta. É preciso saber onde está a informação, durante quanto tempo deve permanecer protegida, que criptografia a protege, por onde circula, quem controla a infraestrutura e quão rapidamente conseguimos alterar os mecanismos de confiança quando o contexto tecnológico muda. Esse é hoje o verdadeiro desafio dos líderes de *segurança*: garantir que a informação continuará protegida enquanto precisar de permanecer confidencial. ◀

por Mauricio Prates,
Network & Security Engineer, Chief Security Officers

CRIPTOGRAFIA PÓS-QUÂNTICA:

PORQUE É PRECISO COMEÇAR A PREPARAR A MIGRAÇÃO

HÁ UMA IDEIA PERIGOSA A CIRCULAR NALGUMAS EQUIPAS DE SEGURANÇA: A DE QUE A CRIPTOGRAFIA PÓS QUÂNTICA PODE ESPERAR ATÉ HAVER UM COMPUTADOR QUÂNTICO CAPAZ DE PARTIR O RSA. O PROBLEMA É QUE, PARA MUITOS DADOS, ESSA ESPERA JÁ CHEGOU TARDE.

Um atacante não precisa de decifrar uma comunicação hoje, basta guardá-la. É a lógica do recolher agora tráfego cifrado, arquivá-lo, e esperar pacientemente que a matemática se torne tratável. Para um contrato comercial que perde valor em dois anos, isso é irrelevante. Para um segredo de estado, um historial clínico ou uma chave de assinatura de longa duração, é um problema muito real, já em curso. Imagine uma empresa que mantém backups cifrados de contratos de aquisição durante 15 anos. Mesmo que o contrato seja inútil daqui a três anos, os dados pessoais e financeiros que o acompanham podem continuar sensíveis durante muito mais tempo.

A razão técnica desta urgência assenta em dois algoritmos quânticos com impactos muito distintos. O algoritmo de Shor resolve de forma eficiente os problemas matemáticos, em que assentam o RSA e a criptografia de curva elíptica (ECC, ECDSA, ECDH). Um computador quântico suficientemente poderoso tornaria computacionalmente viáveis ataques que hoje são impraticáveis contra RSA e criptografia de curva elíptica.


MAURICIO PRATES, CSO

NÃO HÁ UMA DATA CERTA PARA UM COMPUTADOR QUÂNTICO CRIPTOGRAFICAMENTE RELEVANTE. AS ESTIMATIVAS CREDÍVEIS VÃO DE "DENTRO DE UMA DÉCADA" A "TALVEZ NUNCA COM ESTA ARQUITETURA".

Por outro lado, o algoritmo de Grover afeta os algoritmos simétricos e as funções de hash (como o AES ou a família SHA), em termos genéricos, uma aceleração sempre elevada ao quadrado na procura de chaves. Na prática, o ganho é mais complexo, mas constitui uma razão para preferir parâmetros simétricos mais robustos, como AES-256 ao invés do AES-128.

Por isso, o impacto mais disruptivo da computação quântica está hoje associado à criptografia de chave pública. É aqui que entra a criptografia pós-quântica (PQC), também conhecida por quantum-safe. A PQC procura substituir esses mecanismos por algoritmos que podem correr em computadores convencionais, mas cuja segurança assenta em problemas matemáticos para os quais não são conhecidos ataques quânticos eficientes.

O NIST tornou-se uma das principais referências na normalização de PQC, enquanto organismos europeus como a ENISA e o ETSI têm desenvolvido recomendações e especificações próprias para a transição. Em 2024, o NIST fechou a primeira parte desse processo com três normas: ML-KEM para estabelecimento de chaves e ML-DSA e SLH-DSA para assinaturas digitais. Em 2025 acrescentou o HQC como alternativa baseada em códigos, reduzindo a dependência de uma única família matemática.

Comparado com o que já existe, o quadro é assimétrico: RSA e ECC ficam vulneráveis assim que houver capacidade quântica suficiente. AES e as famílias SHA-2/SHA-3 resistem, com parâmetros maiores. Na prática, uma das dificuldades está no tamanho das chaves, assinaturas e mensagens. Em alguns equipamentos, sobretudo IoT e hardware mais antigo, isso pode ser bastante relevante.

A migração deve começar por um inventário criptográfico real: saber onde e como são utilizados RSA e ECC, desde certificados e VPNs até firmware e APIs. É igualmente importante classificar os dados pelo tempo durante o qual precisam de permanecer confidenciais. Sistemas legados, PKI e HSMs raramente foram desenhados para chaves deste tamanho, o que explica a preferência atual por esquemas híbridos, combinando um algoritmo clássico com um pós-quântico no mesmo handshake: se um falhar, o outro ainda protege.

Não há uma data certa para um computador quântico criptograficamente relevante. As estimativas credíveis vão de "dentro de uma década" a "talvez nunca com esta arquitetura". Mas bancos, saúde, telecomunicações e infraestruturas críticas, que guardam dados sensíveis durante décadas, não se podem dar ao luxo de esperar pela certeza. É preciso ter em mente que, com os dados disponíveis hoje, nenhum algoritmo criptográfico, pós-quântico, deve ser tratado como definitivamente seguro. ◀

NetApp

por Tiago Andrade,
Senior Client Executive, NetApp

BRAVE NEW WORLD:

O FUTURO NÃO SERÁ CONQUISTADO PELA TECNOLOGIA. SERÁ DEFINIDO PELA RESILIÊNCIA

A EXPRESSÃO BRAVE NEW WORLD É FREQUENTEMENTE UTILIZADA PARA DESCREVER A CHEGADA DE UMA NOVA ERA. UM MOMENTO DE TRANSFORMAÇÃO PROFUNDA EM QUE AS REGRAS ANTIGAS DEIXAM DE SER SUFICIENTES PARA EXPLICAR UMA REALIDADE INTEIRAMENTE NOVA. NA MINHA PERSPETIVA, É PRECISAMENTE ISSO QUE ESTAMOS A VIVER.

PELA PRIMEIRA VEZ NA HISTÓRIA, A ECONOMIA GLOBAL, AS INFRAESTRUTURAS CRÍTICAS E O FUNCIONAMENTO DAS SOCIEDADES MODERNAS TORNARAM-SE DEPENDENTES DE SISTEMAS DIGITAIS INVISÍVEIS, INTERLIGADOS E EXTRAORDINARIAMENTE COMPLEXOS. ENERGIA, SAÚDE, TRANSPORTES, TELECOMUNICAÇÕES, BANCA, INDÚSTRIA E ADMINISTRAÇÃO PÚBLICA ASSENTAM NUMA BASE TECNOLÓGICA COMUM. O PROBLEMA É QUE ESSA MESMA BASE REPRESENTA HOJE UM DOS MAIORES FATORES DE RISCO SISTÉMICO DO NOSSO TEMPO.

Durante décadas, a transformação digital foi encarada sobretudo como um motor de eficiência, crescimento e inovação. A cloud acelerou a modernização tecnológica. A conectividade reduziu distâncias. A automação aumentou a produtividade. A Inteligência Artificial começou a transformar processos de negócio a uma velocidade sem precedentes.

Mas à medida que avançamos para este novo mundo, emerge uma realidade menos confortável.

Quanto mais dependentes nos tornamos da tecnologia, mais vulneráveis ficamos aos efeitos de uma

AS INFRAESTRUTURAS CRÍTICAS ILUSTRAM ESTA REALIDADE DE FORMA PARTICULARMENTE CLARA. UM OPERADOR ENERGÉTICO DEPENDE DE TELECOMUNICAÇÕES. AS TELECOMUNICAÇÕES DEPENDEM DE ENERGIA. HOSPITAIS DEPENDEM DE AMBAS. TRANSPORTES, SISTEMAS FINANCEIROS E SERVIÇOS DE EMERGÊNCIA DEPENDEM DO FUNCIONAMENTO COORDENADO DE TODOS ESTES ELEMENTOS.

falha. E quando todas as organizações dependem de infraestruturas, plataformas e serviços comuns, o impacto de um incidente deixa de ser local para se tornar sistémico.

É precisamente aqui que surge uma das grandes preocupações da próxima década.

Os riscos sistémicos não são necessariamente causados pelos maiores ataques. Muitas vezes começam com algo aparentemente banal: uma vulnerabilidade num software amplamente utilizado, uma atualização comprometida, um erro humano, uma falha de autenticação ou o comprometimento de um fornecedor crítico.

Numa economia profundamente interligada, uma pequena falha pode desencadear consequências em cadeia difíceis de antecipar.

As infraestruturas críticas ilustram esta realidade de forma particularmente clara. Um operador energético depende de telecomunicações. As telecomunicações dependem de energia. Hospitais dependem de ambas. Transportes, sistemas financeiros e serviços de emergência dependem do funcionamento coordenado de todos estes elementos.

Quando uma disrupção afeta uma destas camadas, rapidamente deixa de ser apenas um problema tecnológico. Pode transformar-se num problema económico, operacional e social.

O verdadeiro desafio não está apenas em proteger sistemas individuais. Está em compreender as dependências invisíveis que ligam organizações, setores e países.

Ao mesmo tempo, uma segunda transformação está silenciosamente a aproximar-se.

A COMPUTAÇÃO QUÂNTICA.

Durante décadas, a confiança digital foi construída sobre mecanismos criptográficos considerados seguros. São eles que protegem transações financeiras, identidades digitais, comunicações privadas e infraestruturas críticas. Contudo,

CAMPANHAS DE ENGENHARIA SOCIAL MAIS CREDÍVEIS, AUTOMAÇÃO DE RECONHECIMENTO, DESENVOLVIMENTO ACELERADO DE MALWARE E OPERAÇÕES CADA VEZ MAIS SOFISTICADAS ESTÃO A ALTERAR PROFUNDAMENTE O EQUILÍBRIO ENTRE DEFESA E ATAQUE.

muitos dos algoritmos atualmente utilizados foram concebidos para um mundo onde a computação quântica não existia.

A grande questão já não é se a computação quântica terá impacto na cibersegurança. A questão é quando esse impacto se tornará relevante.

O risco mais preocupante é aquilo que os especialistas descrevem como Harvest Now, Decrypt Later. Informação recolhida hoje pode ser armazenada durante anos e descodificada no futuro, quando existirem capacidades computacionais suficientes para quebrar os mecanismos criptográficos atuais.

Para governos, operadores de infraestruturas críticas, entidades financeiras e organizações que gerem propriedade intelectual estratégica, este não é um problema teórico. É um desafio de longo prazo que exige preparação imediata.

Mas talvez a transformação mais disruptiva esteja a acontecer ainda mais rapidamente.

A INTELIGÊNCIA ARTIFICIAL.

A IA tem potencial para melhorar significativamente a deteção de ameaças, automatizar operações de segurança e reforçar a capacidade de resposta das organizações. Contudo, também está a aumentar as capacidades dos atacantes.

Campanhas de engenharia social mais credíveis, automação de reconhecimento, desenvolvimento acelerado de malware e operações cada vez mais sofisticadas estão a alterar profundamente o equilíbrio entre defesa e ataque.

Pela primeira vez, assistimos à convergência simultânea de três forças transformadoras: dependência digital crescente, computação quântica e Inteligência Artificial avançada.

É esta combinação que define o verdadeiro significado de Brave New World.

Não estamos apenas perante um novo ciclo tecnológico. Estamos perante uma mudança estrutural na forma como o risco é criado, propagado e amplificado.

Perante esta realidade, a questão já não é saber se uma organização será alvo de um incidente, de uma falha ou de uma disrupção inesperada.

A questão é perceber quão rapidamente conseguirá recuperar.

Porque, no mundo que estamos a construir, a diferença entre liderança e vulnerabilidade deixará de ser determinada pela tecnologia que possuímos.

Será determinada pela resiliência que conseguimos desenvolver. ◀



Fotografias: Rui Santos Jorge

RUI DAMIÃO

"O CISO DEVERÁ SER O MAESTRO E TER A CAPACIDADE DE INTERAGIR COM TODOS"

MIGUEL GONÇALVES

CISO DA VINCI ENERGIES PORTUGAL

MIGUEL GONÇALVES, CISO DA VINCI ENERGIES PORTUGAL, FALA SOBRE A EVOLUÇÃO DO PAPEL DO CISO, A NECESSIDADE DE EQUILIBRAR RISCO E NEGÓCIO E OS DESAFIOS QUE A ADOÇÃO DE INTELIGÊNCIA ARTIFICIAL ESTÁ A TRAZER À CIBERSEGURANÇA.

O Miguel trabalhou cibersegurança dos dois lados, como consultor externo e como CISO interno. Que conselho dava a clientes há alguns anos que sente que, hoje, estava incompleto?

É uma questão muito relevante porque estamos a falar de contextos diferentes. Um consultor externo que chega numa organização não tem, de facto, um conhecimento profundo dessa organização; é uma entidade externa, é alguém independente que leva um conjunto de pessoas, de boas práticas e de ferramentas. No fundo, leva o conhecimento que acabou por obter, fruto da sua experiência de consultoria, porque é uma experiência que acaba por permitir que o profissional tenha um conhecimento bastante heterogéneo dos diferentes verticais do negócio. O que acontece é que este consultor acaba por trazer esse conhecimento para uma organização, mas onde o conhecimento profundo do mesmo sobre a própria não existe.

Diria que há aqui um ponto que é um fator muito diferente. Alguém que chega a uma organização enquanto consultor independente faz uma análise inicial, mas nunca conhece a fundo o próprio contexto da organização, não conhece a fundo a cultura da organização, o estado financeiro da organização e, invariavelmente, acaba por não ter o conhecimento específico que é muito importante ter para poder mitigar riscos.

Quando nós estamos numa organização e trabalhamos internamente para essa organização, há um conhecimento mais profundo que nos permite, muitas das vezes, chegar a conclusões de uma forma mais ágil, porque conhecemos os processos internos e a cultura da organização e esse conhecimento permite-nos tomar decisões e auxiliar na tomada da decisão que estão moldados à organização.

Tendo o privilégio de conhecer os dois lados da moeda, o conselho que daria é que *one size doesn't fit all*. Portanto, não pegarem numa *framework* que é uma *framework* reconhecida ou que possa ser uma *framework* reconhecida internacionalmente, levá-la para uma organização enquanto consultores e tentar que ela caiba naquela cultura.

É muito importante que todos estes projetos de consultoria tenham uma componente de gestão de mudança. A gestão de mudança, quando falamos em segurança de informação, é muito importante, porque estamos a falar em temas que extravasam a pura tecnologia, a pura integração, e esta gestão de mudança e este conhecimento da cultura própria daquela organização vai permitir maior sucesso nos resultados que se pretendem atingir.



As pessoas que entram agora no mercado costumam chegar tecnicamente bem preparadas. Há alguma coisa que a formação académica ou as certificações continuam a não ensinar?

Essa é uma questão também muito pertinente e eu acabo invariavelmente por ter opinião credível sobre essa matéria porque o tema das certificações é um tema que me acompanha. Sabemos que as certificações são extremamente importantes neste mercado, mas é importante dar nota de que uma certificação não é o garante de conhecimento.

A certificação atribui ao profissional um selo que lhe permite trabalhar em determinados meios; não atribui as competências ao profissional. Isto é um aspeto muito importante e, para as gerações mais novas que, saídas da faculdade, têm logo uma ambição muito grande em obterem um conjunto enorme de certificações e colecionarem autênticos álbuns de certificações, é um erro. Muitas das certificações devem ser obtidas no momento certo e devem, no fundo, reforçar e consolidar a experiência que é decaída ao longo dos anos.

No que toca à academia, e este ano vou ter o privilégio de dar aulas tanto no ISCTE como no IPAM sobre estas matérias, a academia está a efetuar um trabalho em Portugal muito interessante relativamente ao tema da segurança de informação.

Durante muitos anos, os profissionais que começaram a trabalhar em segurança de informação e cibersegurança eram sobretudo profissionais que vinham do IT, das tecnologias; o engenheiro informático, o engenheiro eletrotécnico e telecomunicações. O que o mercado e as organizações estão a perceber, e ainda bem, é que o especialista em segurança de informação ou o especialista em cibersegurança não é necessariamente um especialista em tecnologia.

A academia adaptou-se e neste momento já temos uma série de cursos executivos, nomeadamente pós-graduações em diversas faculdades públicas e privadas, já temos licenciaturas e mestrados muito focados na segurança de informação e na cibersegurança. Ou seja, não estão exclusivamente focados no IT,

estão também focados em outras matérias: a gestão, a capacidade de entender e de criar *rapport* com o próximo, a capacidade de saber orquestrar dentro de uma organização áreas heterogéneas – desde um RH a uma área tecnológica, a um C-level.

Esta capacidade que os novos cursos permitem que o aluno saia da faculdade com competências que extravasam a tecnologia. Isto é muitas vezes, ou foi durante muitas vezes, um mito que a cibersegurança e a segurança de informação eram um tema tecnológico e não é e a academia está a adaptar-se nesse sentido.

Há um conjunto de profissionais que está neste momento a formar-se nas faculdades, nos politécnicos, e que acredito que nos próximos anos venha reforçar o nosso mercado, porque de facto, neste momento, ainda há um *gap* grande.

"NÃO VAMOS DIZER QUE A CULTURA SE DEVE SOBREPOR ÀS POLÍTICAS DA ORGANIZAÇÃO, CLARO QUE NÃO, MAS DEVE EXISTIR SENSIBILIDADE POR PARTE DA GESTÃO DE TOPO, POR PARTE DE QUEM DECIDE, PARA QUE AS POLÍTICAS DA ORGANIZAÇÃO TOMEM EM CONSIDERAÇÃO A CULTURA"

Temos muitos especialistas, temos muitos tecnológicos, temos muitos gestores, mas depois há o *gap* para a segurança de informação e da cibersegurança, que no fundo é aqui um *mix* entre estes dois mundos e que, volto a frisar, a academia está a ajustar os seus planos curriculares e está neste momento a promover iniciativas através dos cursos executivos, das pós-graduações, mestrados e licenciaturas, que estão alinhadas com esta necessidade. Vejo que daqui a uns três, quatro, cinco anos, começa a existir aqui um equilíbrio relativamente ao mercado.

Numa organização com a dimensão e complexidade internacional da Vinci Energies, como se equilibra a padronização global de políticas de segurança com as especificidades regulatórias e culturais do mercado português?

Este é um tema que é transversal a todas as organizações e que nos remete para um dos grandes dilemas da segurança de informação neste momento, que é, em muitos casos, a ausência de *governance*.

Temos aqui vários *layers*. Um tema relativamente às políticas da organização, às questões regulatórias e as questões culturais. À data, uma organização tem de conseguir encaixar na sua cultura algo que é uma obrigação. Por outro lado, terá de cumprir com *guidelines* que muitas vezes acabam por surgir numa *perspetiva top-down*, muitas vezes *guidelines* de grupo, e essas *guidelines* têm de ter a capacidade de conseguir absorver as obrigações legais específicas da geografia e serem moldadas à cultura.

Mais uma vez está alinhado com aquilo que disse há pouco e que possivelmente a experiência da consultoria permite ter essa visão, em que nada é estanque.

Quando uma organização tem de cumprir um conjunto de *guidelines* de grupo ou da própria estatutária, naturalmente não as pode colocar em causa, mas tem de tomar em consideração duas coisas: até que ponto é que essas *guidelines* de grupo estão alinhadas com as aglomerações legais? Porque as obrigações legais não têm volta a dar e têm de ser garantidas e a organização e as políticas de organização não se podem sobrepor às obrigações legais.

Por outro lado, não vamos dizer que a cultura se deve sobrepor às políticas da organização, claro que não, mas deve existir sensibilidade por parte da gestão de topo, por parte de quem decide, para que as políticas da organização tomem em consideração a cultura, sem nunca chocar com as obrigações legais.

Isto é um trinómio que aparentemente é simples, mas que requer gestão de mudança, requer uma análise cuidada e pormenorizada, porque qualquer desvio num destes vértices pode provocar um problema grande de organização.

Se o tema da cultura é tomado em consideração em excesso, ou se o tema das políticas torna a organização muito rígida na forma de atuar, ou se existe uma preocupação excessiva com o tema regulatório, então temos aqui desequilíbrio na estrutura da organização. Isso significa que este equilíbrio deve ser mantido através de uma monitorização contínua, seja por ações que tentem manter e preservar a cultura em alinhamento com os princípios e os valores da organização, seja através de um alinhamento constante entre os departamentos de *compliance* e de *legal*.



Qual sente que foi a decisão de segurança mais difícil de 'vender' internamente? Não por ser tecnicamente complexa, mas por exigir mudar comportamentos ou prioridades de pessoas fora da equipa de segurança?

Não vou especificar um problema em concreto, mas sim o tema de uma forma geral. O tema da segurança de informação e tema da cibersegurança – dou sempre esta separação porque são temas diferentes, mas que se complementam e estão de mãos dadas – são temas, para todas as organizações, muitas vezes vistos como um custo. Sendo visto como um custo e não sendo visto como uma área que traga valor financeiro para a organização, não é visto como uma atividade

"O FUTURO CISO TEM DE SER ALGUÉM QUE TENHA SOFT SKILLS PARA CONSEGUIR CRIAR RAPPORT COM OS DIFERENTES ELEMENTOS DE UMA EQUIPA, SEJA UMA EQUIPA DE RESPOSTA A INCIDENTES, SEJA UMA EQUIPA DE MONITORIZAÇÃO, SEJA A GESTÃO DE TOPO"

core; é visto como uma atividade de suporte, o que significa que, em última instância, qualquer tipo de investimento é escrutinado porque as organizações procuram gerar valor.

O tema da segurança de informação e da cibersegurança, durante muitos anos, em muitas organizações, acabava por ser algo que gerava despesa, não valor. O que está a acontecer nas organizações é que há uma sensibilidade muito grande para estes temas, estas matérias, e o tema, já por si, suscita a atenção da gestão de topo e há uma abertura muito grande para estas matérias.

Neste momento, o tema da segurança de informação não é de todo um tema visto como um custo, é visto como uma área extremamente importante e já há uma sensibilidade muito grande, mas é uma questão cultural.

Como é que se mede, na prática, se um investimento em segurança está a valer a pena quando o sucesso é, por definição, a ausência de incidentes?

As coisas têm mudado, mas o que noto, e até na perspetiva enquanto estive do lado da consultoria, é que existem muitos decisores, muitos responsáveis diários que não têm o *pitch* adequado quando tentam vender investimento em cibersegurança.

Vou dar um exemplo. Se efetuar uma alteração na minha plataforma de CRM rapidamente consigo fazer um *business case* e consigo mostrar que com aquela plataforma nova de CRM consigo aumentar o meu número, por exemplo, de acessos, consigo disponibilizar mais soluções aos meus clientes, tenho mais capacidade, logo, potencialmente, vou conseguir aumentar o meu número de vendas. Tenho um *business case* que suporta que aquele investimento poderá vir a trazer retorno em dois, três anos porque é algo que está diretamente associado às atividades *core* da empresa e diretamente associado à capacidade da mesma gerar valor.

Quando decido investir, por exemplo, numa nova firewall, ou quando eu tento instalar uma solução PAM ou IAM, ou o que seja, não consigo fazer este tipo de retorno porque investir nessa solução não vai trazer de forma direta um *business case* para conseguir ter *incoming* financeiro. O que tenho de fazer é ter um *business case* que mostre e que possa evi-

denciar o impacto negativo que a não atualização ou não instalação ou não investimento nessa nova solução pode trazer para a organização.

Cada um saberá do seu negócio e organização, mas é algo muito simples de fazer. Se a minha organização, fruto de um ataque e do não investimento em determinada solução, estiver parada cinco minutos, uma hora, duas horas, 24 horas, uma semana ou um mês, qual é o prejuízo financeiro que vou ter? Depois, qual é o prejuízo reputacional, que é algo muito difícil de quantificar? Quando faço este *business case*, consigo ter estes números – num minuto consigo ter '*x*' de faturação, em cinco minutos terei '*y*' – e é muito fácil justificar que este investimento de 20 ou de 30 mil, que até podia não estar em orçamento, mas que fruto das vulnerabilidades recentes e fruto do que está a acontecer no mercado, tenho mesmo de investir nessa solução para ter uma camada adicional de segurança. Quando vou apresentar a solução e me é dito que não há *budget*, então aí tenho de apresentar estes números e tenho de justificar que estes 30 mil significam para a organização que posso, no limite, não perder dinheiro.

O racional do ROI puro e duro deve ser um pouco invertido. Não o que é que eu vou ganhar financeiramente, agora o que é que eu vou conseguir garantir e preservar para não ter perdas financeiras e reputacionais, que essas são, aí sim, muito difíceis de quantificar.

Nos próximos cinco anos, que competência não técnica vai pesar mais na diferença entre um bom CISO e um CISO apenas tecnicamente competente?

Acima de tudo, e fazendo uma analogia, o CISO deverá ser o maestro. O maestro tem a capacidade de orquestrar aquele conjunto de pessoas, tem a capacidade de conhecer as características de todos os instrumentos, não sendo necessariamente um especialista em todos os instrumentos, poderá em tempos ter sido alguém que tocou determinado instrumento e tem essa capacidade e essa especialização, mas deve ter a capacidade de interagir com todos os músicos, conhecer os instrumentos e identificar as lacunas de cada um e perceber como é que o instrumento A pode trabalhar com o instrumento B.

O futuro CISO tem de ser alguém que tenha *soft skills* para conseguir criar *rapport* com os diferentes elementos de uma equipa, seja uma equipa de resposta a incidentes, seja uma equipa de monitorização, seja a gestão de topo, seja a equipa pura e dura de IT.

Defendo que CISO é um papel que se conquista, ou seja, é-se CISO porque, de facto, há anos de experiência e histórico acumulados porque, acima de tudo, o CISO deve ser alguém que tem a capacidade de orquestrar, mas com conhecimento de causa, que vai transpirar confiança junto do próximo. Transpira-se essa confiança através de conhecimento; quando eu não revelo ter conhecimento, vou criar descrença junto do próximo.

A função de CISO deverá se ruma função de alguém com alguma senioridade, que tenha a expe-



riência, o conhecimento e que tenha, no fundo, esta capacidade de saber orquestrar e ter as tais *soft skills*. Isso é essencial.

Houve alguma decisão ou situação em cibersegurança que o tenha feito mudar de ideias sobre algo em que acreditava firmemente?

A verdade é que, independentemente de existirem normativos, *frameworks*, uma legislação ou diretrizes da empresa, muitas vezes teremos de gerir o risco. Temos de analisar até que ponto a implementação de um ou outro controlo pode chocar com os princípios da organização e a agilidade da organização.

Há uns anos seria mais estanque e mais rígido no cumprimento do normativo ou de uma *framework*, mas nos últimos anos acabei por ser mais ágil e tomar mais em consideração a cultura, as políticas e as diretrizes da organização para fazer cumprir as obrigações legais, mas sem nunca chocar com a agilidade da empresa. Diria que comecei a ter uma visão mais ágil, mais elástica e mais fluída na altura do Regulamento Geral de Proteção de Dados em que, de facto, as organizações começaram a estar muito preocupadas com este tema do RGPD e fomos com as nossas equipas para o terreno e implementar soluções que, em muitos casos, eram bloqueadoras.

Aí confesso que comecei a mudar um pouco a forma de implementar controlos e tomar mais em consideração a cultura da organização e fazer um processo de gestão de mudança mais acompanhado para não nos tornarmos agentes bloqueadores e nos tornarmos agentes de mudança, mas que consigamos manter os níveis de eficiência e de eficácia que são pretendidos na organização.

Geralmente, quando falamos em segurança de informação, cibersegurança, privacidade – curiosamente, quando falamos em Inteligência Artificial [IA] ainda não se fala sobre isso – pensamos que nos vai dar mais trabalho; se estou preocupado com a segurança da privacidade, tenho de fazer mais um ou dois cliques, tenho de percorrer este e aquele *workflow*. Em alguns casos, poderá ser assim. Agora, a forma como embrulhamos a solução e os controlos é que tem de ser inteligente.

Mencionou os controlos e a inteligência artificial. O que sente que vai mudar, numa altura em que temos agentes a comunicar com redes internas e externas e ataques automatizados? O que mais o preocupa?

O tema da IA, este treino da IA, está a trazer aqui um problema, que é, como frisou muito bem, a disseminação de LLM e de agentes de IA por todas as organizações. A IA neste momento é vista de uma maneira em que quem utiliza é alguém que é um visionário; vamos utilizar a IA, vamos acelerar, é fantástico para fazer PowerPoints e para enviar e-mails.

Sou apologista que a nível da academia as coisas vão mudar bastante. Não vamos eliminar, pelo contrário: os alunos devem utilizar IA, as pessoas devem utilizar IA e as organizações devem utilizar IA. Agora, devem utilizá-lo de uma forma controlada. O que está a acontecer neste momento é que essa forma controlada não está a ser adotada. Falando de uma questão mais técnica, uma forma controlada é utilizar um agente dentro de um *tenant* meu. Por exemplo, a Microsoft utiliza o Copilot; no nosso caso, acabamos por ter o nosso *tenant*. Temos um silo onde a informação está ali estanque e não há vazamento de informação. Mas, de facto, com o conjunto de soluções e de agentes que estamos a ver neste momento, há uma utilização não controlada por parte das organizações.

> "A AUSÊNCIA DESTA VISÃO HELICÓPTERO TORNA A VISÃO DO PROFISSIONAL MUITO REDUTORA E MUITO FOCADA NA TECNOLOGIA E AÍ NÃO SE CONSEGUE TER SUCESSO NUMA ORGANIZAÇÃO QUE UTILIZA A TECNOLOGIA COMO SUPORTE, NÃO COMO CORE"

Isto vai nos trazer aqui um problema. Primeiro, perco o controlo de onde está a minha informação e por quem é que ela está a ser utilizada. Segundo, posso atribuir determinado tipo de autonomia a um agente ou um modelo de IA que pode vir a trazer consequências que nem conheço à data.

O tema de IA não é de agora. A IA já existe há muitos anos e já há muitos anos tinha estudado LISP. Agora estamos a falar de outro tipo de IA, que é a IA generativa, que tem a capacidade de se reinventar, que naturalmente não tem ética, não tem sentimentos, mas não sabemos muito bem o que é que poderá vir a acontecer.

Preocupa-me muito que neste momento exista uma utilização desenfreada e não controlada de IA. Os controlos modernos não protegem tudo – até porque não sabemos o que é o tudo –, estamos todos a apalpar terreno e temos um risco muito grande de as organizações perderem por completo o controlo, por um lado, da informação e, por outro, dos agentes que foram construídos.

Há um tema que é uma guerra completamente perdida e que já está a trazer problemas muito grandes na sociedade, questões políticas, económicas e militares, que é a desinformação. Neste momento já ninguém consegue distinguir o que é uma imagem verdadeira ou o que é um vídeo falso.

Como é que as organizações o podem combater: com políticas restritas relativamente à utilização do IA, com regras claras, com *awareness*, com sensibilização e com formação. Vai ser suficiente? Acho que não.

Que conselho dá a quem está a começar hoje em cibersegurança?

Tenho dado estes conselhos quase diariamente ao meu filho que quer seguir esta área e é um bom exemplo. Os miúdos que neste momento começam a pensar em trabalhar na cibersegurança pensam muito em hacking, nos pen testing, em trabalhar com blockchain, na IA. Mais uma vez, tem uma visão muito tecnológica. A cibersegurança é um tema da sociedade, é um tema social, é, acima de tudo, um tema que envolve políticas, processos e pessoas e tecnologia, naturalmente.

O grande conselho que dou para quem quer trabalhar nesta área é que é importante especializarem-se e terem a sua formação numa base tecnológica para conseguirem ter um entendimento do ecossistema da segurança de informação e da cibersegurança, mas deverão também ter formação – pode ser através da sua licenciatura, pode ser depois de uma pós-graduação – em gestão de sistemas de informação. Isso é muito importante, porque esta capacidade de ter uma visão helicóptero é necessária na segurança de informação e é essencial para o sucesso do profissional. A ausência desta visão helicóptero torna a visão do profissional muito redutora e muito focada na tecnologia e aí não se consegue ter sucesso numa organização que utiliza a tecnologia como suporte, não como *core* e que, em cima de tudo, é constituída por pessoas.



O conselho é não se limitar à tecnologia, fazer a sua formação académica em cursos que são permanentemente tecnológicos, mas depois tentar encontrar outros caminhos, nomeadamente através de pós-graduações ou mestrados.

Não obstante, como eu há pouco já dizia, as licenciaturas em cibersegurança neste momento já trazem também esses *add-ons* e já capacitam os mais novos em temas que extravasam a tecnologia.

NUNO GOES, CYBERSECURITY ENGINEER, É ESPECIALISTA EM SEGURANÇA DE INFORMAÇÃO E CIBERSEGURANÇA, COM UMA EXTENSA EXPERIÊNCIA NESTE SETOR. DOCENTE UNIVERSITÁRIO E FORMADOR. BOARD MEMBER DA CIIWA, COORDENA O GRUPO DE TRABALHO ESPECIALIZADO EM SEGURANÇA DA INFORMAÇÃO.



POR • NUNO GOES, CYBERSECURITY ENGINEER

47 DIAS:

O PRAZO QUE VAI OBRIGAR AS ORGANIZAÇÕES A AUTOMATIZAR A CONFIANÇA DIGITAL

EM ABRIL DE 2025, O CA/BROWSER FORUM APROVOU, POR UNANIMIDADE ENTRE AUTORIDADES DE CERTIFICAÇÃO E FABRICANTES DE BROWSERS, A BALLOT SC-081V3 . A DECISÃO PARECE TÉCNICA, MAS VAI ATINGIR TODAS AS ORGANIZAÇÕES COM PRESENÇA ONLINE: A VALIDADE MÁXIMA DOS CERTIFICADOS TLS PÚBLICOS, DE 398 DIAS, CAI PARA 200 DIAS EM MARÇO DE 2026, 100 EM MARÇO DE 2027 E APENAS 47 EM MARÇO DE 2029.

Para quem gere dezenas ou centenas de certificados, a mudança é mais profunda do que parece à primeira vista. Renovar um certificado uma vez por ano, com um processo manual e um aviso no calendário, sempre foi tolerável e exequível. Renovar o mesmo certificado sete ou oito vezes por ano, multiplicado por centenas de ativos espalhados por servidores, balanceadores de carga, APIs e dispositivos, já não é um problema de gestão rotineira: é um problema de escala. Uma organização com mil certificados públicos, que hoje faz duas ou três renovações

por mês, vai precisar de cerca de vinte operações por dia útil quando o limite atingir 47 dias. Quem já geriu um parque de certificados sabe como um único esquecimento pode tirar um serviço do ar. Sem automação de ponta a ponta, deixa de ser uma questão de "se" e passa a ser uma questão de "quando" um certificado expirado vai tornar indisponível algo importante ou impactar o rate de segurança da organização.

Para além do aspeto técnico, é um tema que abrange automatização, maturidade processual, conformidade legal, governance, e até a soberania digital, com impacto na operação e resiliência.

É por isso que a automatização do ciclo de vida dos certificados deixa de ser uma boa prática e passa a ser uma condição de sobrevivência operacional, exigindo um nível mais elevado de maturidade. O protocolo ACME (RFC 8555), criado para uso na Let's Encrypt, é hoje suportado pela maioria das autoridades de certificação comerciais e permite solicitar, validar, instalar e renovar certificados sem intervenção humana. Mas, por si só, resolve apenas parte do problema. Uma automatização integrada começa pela identificação: a maior parte das organizações subestima quantos certificados têm em produção, porque muitos foram emitidos ao longo dos anos por equipas diferentes, fora de qualquer inventário central. Só depois de mapear esse parque faz sentido escolher uma plataforma de Certificate Lifecycle Management, capaz de gerir pedidos, distribuir certificados aos pontos certos e revogar automaticamente os que já não são necessários. Essa orquestração deve estar ligada aos pipelines de CI/CD, para que um novo serviço nasça já com o certificado correto, e deve incluir alertas com semanas de antecedência, não horas, quando uma renovação falhar silenciosamente. Vista assim, a redução para 47 dias tem um efeito colateral positivo: obriga a tratar a gestão de certificados como infraestrutura crítica automatizada, reduzindo a janela de exposição em caso de compromisso de uma chave privada.

Importa clarificar um ponto frequentemente mal interpretado: esta obrigação aplica-se apenas a certificados públicos, emitidos por autoridades de certificação reconhecidas pelos browsers. Certificados

"UM ESTADO OU UM SETOR CRÍTICO CUJA CONTINUIDADE DE SERVIÇO PASSA A DEPENDER, A CADA SEIS OU SETE SEMANAS, DE UMA AUTORIDADE DE CERTIFICAÇÃO ESTRANGEIRA ESTÁ A ASSUMIR UM RISCO QUE ULTRAPASSA O PLANO TÉCNICO. PODE OCORRER POR MEIO DE SANÇÕES, RESTRIÇÕES COMERCIAIS OU SIMPLES DECISÕES DE NEGÓCIOS DE UM FORNECEDOR QUE, EM TEORIA, PODEM CONDICIONAR A PRESTAÇÃO DE SERVIÇOS ESSENCIAIS".

emitidos por autoridades de certificação internas ou privadas, típicos de ambientes corporativos fechados, permanecem fora do âmbito das regras do CA/Browser Forum. As organizações mantêm a liberdade para definir a validade desses certificados internos, o que não as dispensa de rever a sua própria política de gestão de chaves à luz do que está a mudar no exterior.

Há, porém, uma dimensão que ultrapassa a operação técnica. A maioria das autoridades públicas de certificação mais usadas na Europa (como a DigiCert, Sectigo, GlobalSign, etc.) está sediada fora da União Europeia, sobretudo nos Estados Unidos. Um ciclo de renovação que passa a exigir contacto quase contínuo com essas entidades, muitas vezes através de infraestrutura que a organização não controla, aprofunda uma dependência já hoje discutida em termos de soberania digital. Um Estado ou um setor crítico cuja continuidade de serviço passa a depender, a cada seis ou sete semanas, de uma autoridade de certificação estrangeira está a assumir um risco que ultrapassa o plano técnico. Pode ocorrer por meio de sanções, restrições comerciais ou simples decisões de negócios de um fornecedor que, em teoria, podem condicionar a prestação de serviços essenciais. A União Europeia tenta colmatar esta lacuna com os QWAC previstos no eIDAS , mas a adoção destes certificados qualificados europeus está longe de ser a norma.

É aqui que a questão deixa de ser apenas de engenharia e passa a ser de conformidade regulatória. O artigo 21.º da NIS2 obriga as entidades essenciais e importantes a adotar medidas de gestão do risco que incluem políticas de criptografia, segurança da cadeia de abastecimento e continuidade do negócio, áreas nas quais a gestão do ciclo de vida de certificados públicos se insere diretamente. Um certificado que expira sem aviso prévio pode gerar um incidente de disponibilidade com potencial de notificação obrigatória às autoridades competentes. No setor financeiro, o DORA segue uma lógica semelhante ao exigir uma gestão robusta do risco de TIC e das dependências de terceiros, incluindo fornecedores críticos, como as autoridades de certificação. Uma matriz do risco que ainda trate os certificados TLS como um detalhe de infraestrutura, em vez de um ativo a monitorizar e reportar, vai ficar rapidamente desadequada.

Em conclusão, o prazo até 2029 pode parecer longo, mas o primeiro corte, para 200 dias, já está em vigor desde março de 2026, e o seguinte é já em março de 2027. Entre um limite e outro não sobra muito tempo para reagir de forma improvisada. Três frentes merecem prioridade imediata:

- um inventário completo e centralizado de todos os certificados públicos em produção, incluindo os emitidos fora de qualquer processo formal;

- um plano de automatização assente em ACME e numa plataforma de gestão do ciclo de vida, integrado com os processos de DevOps;

- e a integração explícita deste risco nos programas de conformidade com a NIS2 e, quando aplicável, com DORA, avaliando a exposição a autoridades de certificação estrangeiras como risco de terceiros.

As organizações que assumirem esta mudança como uma oportunidade de modernizar e reforçar a sua confiança digital vão chegar a 2029 preparadas. As que continuarem a tratar o tema como mero detalhe técnico a resolver mais tarde, vão descobrir, mais cedo do que gostariam, que 47 dias passam muito depressa...

NUNO REIS É CYBER SECURITY OFFICER NA ROBERT BOSCH, S.A., COM FOCO EM CIBERSEGURANÇA E COORDENAÇÃO INTERNACIONAL DE CYBER SECURITY OFFICERS. COMPLEMENTA A SUA ATUAÇÃO NAS ÁREAS DE SEGURANÇA DA INFORMAÇÃO E ACCESS MANAGEMENT. É ESPECIALISTA EM CIBERSEGURANÇA PELA ACADEMIA NACIONAL DE CIBERSEGURANÇA E AUDITOR ISO 27001 CERTIFICADO PELA AENOR.



TUDO ESTÁ LIGADO. NEM TUDO ESTÁ PROTEGIDO.

POR NUNO REIS,
CYBER SECURITY OFFICER NA ROBERT BOSCH, S.A.

NA CIBERSEGURANÇA, CONTINUAMOS MUITAS VEZES A PENSAR EM COMPUTADORES, SERVIDORES, REDES E UTILIZADORES, MAS O PERÍMETRO MUDOU HÁ MUITO TEMPO.

Hoje, televisões, câmaras, lâmpadas, assistentes de voz, relógios, eletrodomésticos, sensores, sistemas de climatização e muitos outros equipamentos estão ligados à Internet. Chamamos-lhes dispositivos inteligentes. A questão é saber quão inteligentes continuam quando olhamos para a segurança.

Um dispositivo simples também é um computador.

Por detrás de uma câmara, de uma lâmpada ou de um assistente de voz existem software, firmware, interfaces de rede, mecanismos de autenticação e, muitas vezes, serviços cloud.

Ou seja, existe uma superfície de ataque.

O NIST identifica capacidades como identificação do dispositivo, configuração segura, proteção de dados, controlo de acesso e atualização de software como parte de uma linha de base de cibersegurança para dispositivos IoT.

O problema é que nem todos os dispositivos foram concebidos, adquiridos ou mantidos com esse nível de exigência.

O RISCO COMEÇA NO CICLO DE VIDA

Num computador empresarial, uma vulnerabilidade tende a entrar num processo conhecido: é identificada, avaliada, priorizada e corrigida.

Num dispositivo IoT, a realidade pode ser muito diferente.

Quem sabe que versão de firmware está instalada numa câmara comprada há quatro anos? O fabricante continua a publicar atualizações? O equipamento atualiza automaticamente? Existe alguém responsável por verificar isso?

Para mim, este é um dos riscos mais subestimados no IoT: o dispositivo continua a funcionar, mas a sua vida útil de cibersegurança pode já ter terminado.

Uma televisão pode continuar a funcionar perfeitamente e, ao mesmo tempo, deixar de ser um equipamento que queremos manter na mesma rede onde existem sistemas mais sensíveis.

TUDO LIGADO SIGNIFICA MAIS DEPENDÊNCIAS

Nem todos os equipamentos IoT estão diretamente expostos à Internet, e é importante não simplificar demasiado esta questão.

Mas quanto mais dispositivos ligamos, mais relações de confiança criamos.

Uma câmara comunica com um serviço cloud. Um assistente de voz envia pedidos para processamento remoto. Um eletrodoméstico depende de uma aplicação móvel e de APIs externas. Uma lâmpada utiliza Wi-Fi, Bluetooth ou um hub.

Cada ligação acrescenta dependências.

E cada dependência deveria obrigar a perguntas básicas: quem comunica com quem, através de quê, com que autenticação, que dados são tratados e durante quanto tempo aquele produto continuará a ser suportado?

PASSWORDS ANTIGAS EM DISPOSITIVOS NOVOS

Há riscos no IoT que não são novos. A autenticação é um bom exemplo.

"POR DETRÁS DE UMA CÂMARA, DE UMA LÂMPADA OU DE UM ASSISTENTE DE VOZ EXISTEM SOFTWARE, FIRMWARE, INTERFACES DE REDE, MECANISMOS DE AUTENTICAÇÃO E, MUITAS VEZES, SERVIÇOS CLOUD. OU SEJA, EXISTE UMA SUPERFÍCIE DE ATAQUE".

Credenciais por defeito, passwords fracas ou mecanismos de autenticação mal implementados continuam a transformar dispositivos aparentemente inofensivos em pontos de entrada desnecessários.

A ETSI EN 303 645 estabelece, para IoT de consumo, que as passwords não devem ser universais por defeito, refletindo uma lição básica: tecnologia nova não elimina problemas antigos. Muitas vezes apenas os desloca para outro dispositivo.

Mudar credenciais por defeito, utilizar autenticação forte e desativar serviços desnecessários continuam a ser medidas simples, mas relevantes.

"A SEGMENTAÇÃO DE REDE CONTINUA, POR ISSO, A SER UMA DAS FORMAS MAIS EFICAZES DE LIMITAR O IMPACTO DE UM EQUIPAMENTO COMPROMETIDO.
UMA LÂMPADA INTELIGENTE, UMA TELEVISÃO OU UMA CÂMARA NÃO DEVERIAM TER ACESSO DESNECESSÁRIO A SISTEMAS CRÍTICOS APENAS PORQUE PARTILHAM A MESMA INFRAESTRUTURA.
O PRINCÍPIO É SIMPLES: ASSUMIR QUE UM DISPOSITIVO PODE FALHAR E LIMITAR AQUILO QUE CONSEGUE ALCANÇAR QUANDO ISSO ACONTECE".

O PROBLEMA DOS DISPOSITIVOS ESQUECIDOS

Talvez o maior desafio não seja o dispositivo que acabámos de instalar.

É aquele que instalámos há anos e que ninguém se recorda.

Uma câmara numa sala, um sensor num armazém, uma televisão numa área comum, uma impressora, um sistema de videoconferência ou um equipamento instalado por um fornecedor podem permanecer ligados muito para além do período em que alguém acompanha ativamente a sua segurança.

Se não existir inventário, ownership e gestão de ciclo de vida, surge uma pergunta desconfortável: como protegemos aquilo que nem sequer sabemos que está ligado?

É aqui que asset management deixa de ser apenas uma tarefa administrativa. Passa a ser um controlo de cibersegurança.

SEGMENTAR PARA LIMITAR O IMPACTO

Nem todos os dispositivos precisam de comunicar com todos os sistemas.

A segmentação de rede continua, por isso, a ser uma das formas mais eficazes de limitar o impacto de um equipamento comprometido.

Uma lâmpada inteligente, uma televisão ou uma câmara não deveriam ter acesso desnecessário a sistemas críticos apenas porque partilham a mesma infraestrutura.

O princípio é simples: assumir que um dispositivo pode falhar e limitar aquilo que consegue alcançar quando isso acontece.

O FATOR HUMANO CONTINUA PRESENTE

Também no IoT, o fator humano está no centro.

Somos nós que ligamos os dispositivos, aceitamos configurações por defeito, adiamos atualizações, instalamos aplicações e concedemos permissões.

Mas isto não significa que o utilizador seja o problema.

Significa que produtos e processos devem ser desenhados para não depender de comportamentos perfeitos: atualizações seguras, configurações robustas por defeito, autenticação adequada, informação clara sobre suporte e mecanismos simples de gestão.

Segurança tem de acompanhar o produto ao longo da sua vida, e não apenas até ao momento em que sai da caixa.

ESTAR LIGADO É UMA DECISÃO DE RISCO

A resposta não é deixar de utilizar IoT.

A tecnologia traz eficiência, automação, conforto e novas capacidades. O problema começa quando "ligar à Internet" é tratado apenas como uma funcionalidade e não como uma decisão de risco.

"A TECNOLOGIA TRAZ EFICIÊNCIA, AUTOMAÇÃO, CONFORTO E NOVAS CAPACIDADES. O PROBLEMA COMEÇA QUANDO "LIGAR À INTERNET" É TRATADO APENAS COMO UMA FUNCIONALIDADE E NÃO COMO UMA DECISÃO DE RISCO."

Antes de ligar mais um equipamento, talvez devêssemos fazer algumas perguntas simples:

Precisa mesmo de estar ligado?

Quem o vai gerir?

Como será atualizado?

Durante quanto tempo terá suporte?

O que acontece quando deixar de o ter?

A que outros sistemas consegue chegar?

Num mundo onde quase tudo pode estar conectado, o verdadeiro desafio não é ligar mais dispositivos.

É garantir que continuamos a saber o que está ligado, porquê, quem é responsável e até quando conseguimos protegê-lo. ◀

PAULO MARTINS É DIRETOR DE TI E OPERAÇÕES DO SPORT LISBOA E BENFICA, COM MAIS DE 25 ANOS DE EXPERIÊNCIA EM TECNOLOGIA, CIBERSEGURANÇA, INFRAESTRUTURAS, MEDIA E TRANSFORMAÇÃO DIGITAL. ESPECIALISTA EM LIDERANÇA DE EQUIPAS E OPERAÇÕES CRÍTICAS, ALIA VISÃO ESTRATÉGICA, INOVAÇÃO E RESILIÊNCIA NA TRANSFORMAÇÃO E EVOLUÇÃO DE ECOSSISTEMAS TECNOLÓGICOS COMPLEXOS.



POR PAULO MARTINS,
DIRETOR DE TI E OPERAÇÕES DO SPORT LISBOA E BENFICA

OPERAÇÕES DE TI NA ERA DA INTELIGÊNCIA ARTIFICIAL

A INTELIGÊNCIA ARTIFICIAL ESTÁ A DEIXAR DE SER UMA TECNOLOGIA EXPERIMENTAL PARA SE TORNAR UMA COMPONENTE INTEGRADA NA FORMA COMO AS ORGANIZAÇÕES TRABALHAM.

O seu impacto é particularmente evidente nas operações de Tecnologias de Informação (TI), onde a quantidade de sistemas, dados, utilizadores e dependências tecnológicas cresce continuamente.

Durante muitos anos, as equipas de TI concentraram-se em manter a infraestrutura disponível, responder a incidentes e resolver problemas à medida que iam surgindo. Hoje, essa missão mantém-se, mas o contexto mudou. As organizações esperam operações mais rápidas, eficientes, resilientes e capazes de antecipar falhas. É neste cenário que a inteligência artificial pode desempenhar um papel decisivo.

As plataformas de monitorização já recolhem grandes volumes de informação sobre aplicações, redes, servidores, serviços cloud e dispositivos. A IA permite analisar estes dados em tempo real, identificar padrões anómalos e relacionar acontecimentos que, isoladamente, poderiam parecer irrelevantes. Uma degradação gradual do desempenho, um aumento invulgar de pedidos ou alterações no comportamento de uma aplicação podem, assim, ser detetados antes de provocarem uma interrupção do serviço.

Esta capacidade favorece uma mudança importante: passar de uma atuação reativa para uma operação mais preditiva. Em vez de esperar que um sistema falhe para intervir, as equipas podem antecipar problemas, prever necessidades de capacidade e programar ações de manutenção com menor impacto no negócio.

A eficiência é igualmente relevante nas operações de segurança. Os centros de operações de segurança enfrentam diariamente milhares de alertas, muitos dos quais repetidos, pouco relevantes ou sem consequências reais. A IA pode correlacionar eventos, eliminar parte do ruído, identificar padrões de ataque e atribuir prioridades com base no risco efetivo para a organização. Desta forma, os analistas deixam de despender tanto tempo na triagem manual e podem concentrar-se nos incidentes que exigem conhecimento especializado e decisão humana.

Na investigação de incidentes, a IA permite reunir informação proveniente de diferentes ferramentas, reconstruir uma sequência de acontecimentos e apresentar um resumo claro do ocorrido. Consegue ainda sugerir hipóteses, procurar indicadores relacionados e apoiar a produção de relatórios. O resultado esperado é uma redução do tempo de deteção e de resposta, bem como uma utilização mais eficiente dos recursos disponíveis.

A automatização possibilita também executar ações previamente definidas, como bloquear um endereço suspeito, isolar um equipamento ou suspender temporariamente uma conta comprometida. Estas medidas podem limitar a propagação de um ataque nos primeiros minutos, quando a rapidez é determinante. No entanto, devem ser aplicadas com critérios claros e proporcionais ao risco. Uma decisão incorreta pode interromper operações legítimas ou causar impactos significativos no negócio.

A inteligência artificial generativa acrescenta uma nova dimensão a este processo. Os profissionais podem utilizá-la para pesquisar documentação, resumir incidentes, produzir relatórios, criar scripts, explicar mensagens de erro ou apoiar a análise de configurações. Isto pode reduzir significativamente

"A INTELIGÊNCIA ARTIFICIAL GENERATIVA ACRESCENTA UMA NOVA DIMENSÃO A ESTE PROCESSO. OS PROFISSIONAIS PODEM UTILIZÁ-LA PARA PESQUISAR DOCUMENTAÇÃO, RESUMIR INCIDENTES, PRODUZIR RELATÓRIOS, CRIAR SCRIPTS, EXPLICAR MENSAGENS DE ERRO OU APOIAR A ANÁLISE DE CONFIGURAÇÕES".

o tempo gasto na procura de informação e facilitar a colaboração entre equipas de TI e de segurança.

Contudo, a adoção de IA não consiste apenas em instalar novas ferramentas. Exige uma transformação dos processos e da própria organização do trabalho. As equipas terão de rever procedimentos, melhorar a qualidade dos dados, documentar o conhecimento existente e definir claramente quais as decisões que podem ser automatizadas e quais devem continuar a depender de validação humana.

A preparação das pessoas será igualmente determinante. Os profissionais de TI não deixarão de ser necessários, mas terão de desenvolver novas competências. A capacidade de interpretar dados, avaliar recomendações, compreender o funcionamento dos modelos e questionar resultados será tão importante como o conhecimento técnico tradicional. Competências de comunicação, pensamento crítico e compreensão do negócio ganharão também maior relevância.

Existem riscos que devem ser considerados desde o início. Uma recomendação incorreta pode provocar indisponibilidade de serviços, perda de dados ou alterações indevidas num ambiente de produção. A utilização de informação sensível em ferramentas de IA pode criar problemas de confidencialidade. Modelos treinados com dados incompletos ou pouco representativos podem produzir resultados inadequados.

A segurança deve estar presente em todas estas etapas. À medida que aumenta a automatização, torna-se fundamental proteger identidades, acessos privilegiados, interfaces entre sistemas e os próprios modelos de IA. A tecnologia que ajuda a gerir a infraestrutura pode também tornar-se um alvo ou ser explorada para causar impacto em maior escala.

As organizações devem começar por problemas concretos, como a redução de alertas duplicados, a diminuição do tempo de resolução de incidentes ou a automatização de tarefas de baixo risco. Os resultados devem ser medidos através de indicadores claros, como disponibilidade, tempo de resposta, número de incidentes evitados, eficiência das equipas e satisfação dos utilizadores.

A IA não substituirá as operações de TI, mas modificará profundamente a forma como são concebidas e executadas. As equipas que conseguirem combinar automatização, conhecimento técnico e supervisão humana estarão mais bem preparadas para responder às exigências de um ambiente cada vez mais digital.

Na era da inteligência artificial, o verdadeiro desafio não é apenas adotar novas ferramentas: é repensar a forma como as organizações operam, tomam decisões e desenvolvem as competências necessárias para trabalhar com a tecnologia de forma segura, responsável e eficiente. ◀

▼
"A SEGURANÇA DEVE ESTAR PRESENTE EM TODAS ESTAS ETAPAS. À MEDIDA QUE AUMENTA A AUTOMATIZAÇÃO, TORNA-SE FUNDAMENTAL PROTEGER IDENTIDADES, ACESSOS PRIVILEGIADOS, INTERFACES ENTRE SISTEMAS E OS PRÓPRIOS MODELOS DE IA".

CYBER BLUEPRINT PARA LÁ DAS FRONTEIRAS

Ilustração de macrovector - Magnific.com

POR INÊS GARCIA MARTINS

UM SISTEMA FALHA, O INCIDENTE ALASTRA E, DE REPENTE, JÁ NÃO HÁ UMA ÚNICA ORGANIZAÇÃO A RESPONDER. QUANDO UMA CIBERCRISE ATRAVESSA SETORES E FRONTEIRAS, COORDENAR DECISÕES, INFORMAÇÃO E COMUNICAÇÃO TORNA-SE PARTE DA PRÓPRIA RESPOSTA.

Um ciberincidente pode começar dentro de uma organização e, em pouco tempo, ultrapassar sistemas, setores e fronteiras. Quando o impacto deixa de poder ser gerido por uma única entidade ou Estado, a resposta já não depende apenas da capacidade técnica para conter o ataque. Exige coordenação entre organizações, autoridades e estruturas europeias. É esse o problema que o *Cyber Blueprint* procura responder.

Adotado pelo Conselho da União Europeia em junho de 2025 sob a forma de uma recomendação, o *Cyber Blueprint* é um documento orientador para a gestão europeia de cibercrises, concebido para clarificar como os diferentes atores devem interagir na preparação e resposta a incidentes de cibersegurança de grande escala e cibercrises. Não cria obrigações novas para as organizações nem novas estruturas de resposta. Define antes como devem interagir os mecanismos existentes e como se articulam os níveis técnico, operacional e político ao longo da gestão de uma crise. O documento atualiza o enquadramento europeu de 2017 e incorpora a arquitetura entretanto criada por instrumentos como a NIS2 e o *Cyber Solidarity Act*.

"O objetivo não é criar estruturas, mas tornar utilizáveis e coordenados os mecanismos já existentes", explica Elsa Lemos, especialista em comunicação de crise. É, sobretudo, "uma questão de coordenação".

A necessidade dessa coordenação resulta da própria dimensão que uma cibercrise pode assumir. Para a especialista, a Comissão parte da constatação de que "um incidente de cibersegurança pode ultrapassar rapidamente as fronteiras de uma organização, de um setor e de um Estado-Membro". A partir daí, pode "produzir efeitos de alto impacto em funções essenciais da sociedade e contaminar outros Estados. Podemos estar a falar de riscos de segurança, riscos económicos ou outros".

Na origem desta recomendação está também aquilo que Elsa Lemos identifica como uma "fal-

ta de visão operacional comum sobre quem faz o quê quando uma cibercrise ultrapassa as fronteiras". Perante este cenário, considera "mandatório existir algo que coloca os pontos nos i's" e clarifica a articulação entre os diferentes intervenientes.

ESCALAR ANTES DE CONHECER TUDO

Reconhecer quando um incidente deixa de poder ser tratado exclusivamente dentro de portas é um dos primeiros desafios para as organizações. Na visão de Miguel Gonçalves, CISO da CUF, "essa fronteira não é determinada pela dimensão técnica do incidente. É ultrapassada quando percebemos que o impacto, ou o potencial impacto, deixou de estar exclusivamente sob o controlo da nossa organização".

Na saúde, essa mudança pode acontecer rapidamente. Um incidente inicialmente circunscrito a um sistema ou infraestrutura tecnológica pode evoluir para um problema de continuidade de cuidados, com impacto em doentes, profissionais, fornecedores ou outras entidades do setor. É também por isso que, segundo o responsável, "não podemos esperar por conhecer toda a dimensão do incidente para começar a escalar".


MIGUEL GONÇALVES, CUF

Numa fase inicial, explica, a organização trabalha com indicadores, informação incompleta e perguntas ainda sem resposta. É neste contexto inevitavelmente imperfeito, e antes de existir uma fotografia completa do incidente, que a decisão de escalar tem de ser tomada. Sinais de propagação, dependências críticas, impacto relevante ou potenciais efeitos noutras organizações podem ser suficientes para iniciar

> "ESPERAR POR TER TODAS AS RESPOSTAS ANTES DE PEDIR AJUDA OU PARTILHAR INFORMAÇÃO É PROVAVELMENTE UMA BOA FORMA DE CHEGAR ATRASADO À CRISE"


ELSA LEMOS, ESPECIALISTA EM COMUNICAÇÃO DE CRISE

a coordenação. Como sintetiza Miguel Gonçalves, "esperar por ter todas as respostas antes de pedir ajuda ou partilhar informação é provavelmente uma boa forma de chegar atrasado à crise".

Quando a resposta envolve várias entidades, surge ainda o problema de construir uma visão comum do que está a acontecer. Elsa Lemos chama a atenção para a necessidade de uma *shared situational awareness*, uma vez que diferentes entidades "podem estar a trabalhar com visões distintas da situação e podem tomar decisões corretas a nível local, mas incoerentes a nível europeu".

"A ORGANIZAÇÃO DEVE PREPARAR-SE PARA OPERAR NUM AMBIENTE ONDE A COMUNICAÇÃO É PARTE DA RESPOSTA ESTRATÉGICA"

RAPIDEZ EM TEMPO DE CRISE

Quanto maior a crise, maior é a necessidade de fazer circular informação. Porém, numa crise, a urgência em fazer circular informação pode entrar em conflito com a necessidade de a validar. "Temos de ser rápidos, mas não podemos transformar uma hipótese num facto", sintetiza Miguel Gonçalves. A resposta passa por distinguir claramente aquilo que a organização sabe, aquilo que considera poder estar a acontecer e aquilo que ainda desconhece.

Para o CISO da CUF, "as relações de confiança e os canais de comunicação constroem-se antes do incidente. Durante a crise precisamos simplesmente que funcionem". Nesse sentido, autoridades, parceiros críticos e outras organizações do setor devem conhecer previamente os interlocutores, canais e informação que podem vir a ter de partilhar.

O problema pode começar nos próprios meios usados para coordenar a resposta. Elsa Lemos identifica a "indisponibilidade de canais de comunicação" como uma das vulnerabilidades a considerar, perante a possibilidade de perturbação ou falha das redes normais de telecomunicações e Internet durante uma crise severa.

O *Cyber Blueprint* inclui a comunicação segura entre as áreas a desenvolver. A recomendação prevê que a Comissão proponha, até ao final de 2026, um conjunto interoperável de soluções de comunicação segura, abrangendo voz, dados, videoconferência, mensagens, colaboração e partilha documental. O acordo entre Conselho, Comissão, Alto Representante, EU-CyCLONe e Rede de CSIRT sobre esse conjunto está previsto até ao final de 2027.

Garantir os canais, porém, não resolve todo o problema. Elsa Lemos identifica também como riscos "a desinformação" e as "mensagens contraditórias" ou pouco alinhadas entre entidades, Estados ou instituições europeias. A preparação passa, na sua perspetiva, por uma "Estratégia de Comunicação Pública Coordenada" e por exercícios conjuntos que permitam testar a articulação entre setores civis, militares e privados.

Esta dimensão ganha importância quando os efeitos deixam de ser apenas tecnológicos. Elsa Lemos considera que "uma cibercrise é multidimensional" e defende uma lógica *whole-of-government*, *whole-of-society* e *all-hazards*. Os impactos podem chegar à economia, às infraestruturas críticas, à segurança, à defesa e às relações internacionais.

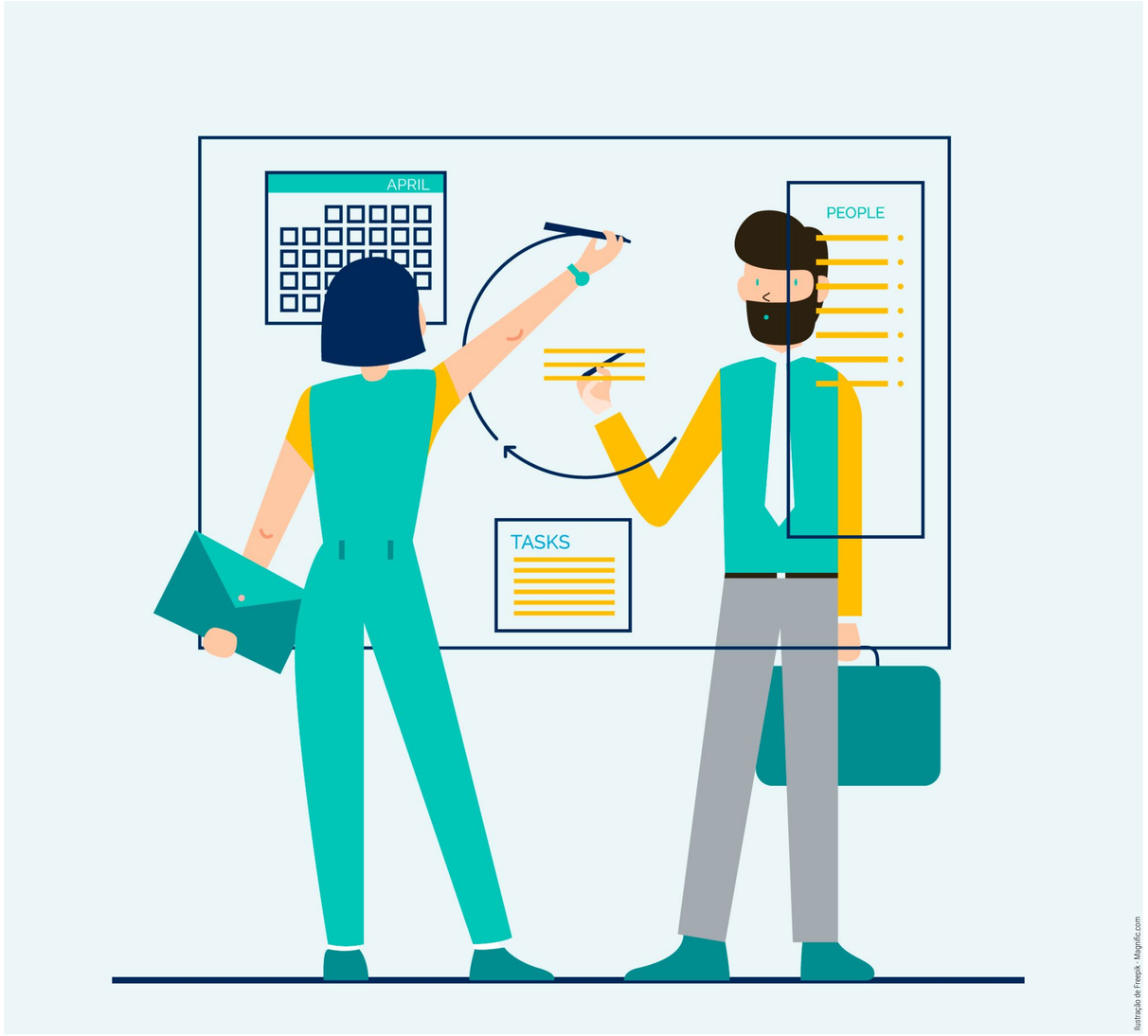


Ilustração de Freepik - Magnific.com

QUEM RESPONDE QUANDO A CRISE CRESCE

O *Cyber Blueprint* diz-nos que quando um incidente ganha dimensão, as organizações continuam responsáveis pela sua resposta, mas passam a ter de lidar com uma rede mais complexa de obrigações e autoridades. Ricardo Henriques, sócio da Abreu Advogados, considera, por isso, importante "distinguir, por um lado, o plano da gestão do incidente pela organização, e, por outro, a coordenação da resposta pelas autoridades".

A complexidade aumenta num quadro regulatório europeu em que o mesmo incidente pode desencadear obrigações de reporte ao abrigo de diferentes regimes. A NIS2, o RGPD ou o DORA podem obrigar uma organização a comunicar o mesmo acontecimento a diferentes destinatários, com prazos e requisitos distintos, precisamente quando a informação disponível "ainda é incompleta e está sujeita a revisão", como salienta Ricardo Henriques.

De acordo com Ricardo Henriques, "os próprios processos de reporte, e em especial os canais de entrada de informação, estão em revisão ao nível europeu". A proposta de Digital Omnibus, apresentada em novembro de 2025, pretende alterar a NIS2, o RGPD e o DORA e criar um ponto único de entrada para as notificações. Entre as alterações propostas está também a extensão para 96 horas do prazo de notificação de violações de dados pessoais.

O desafio seguinte refere-se à implementação nacional, garantindo que esse canal único permite transmitir a informação de forma segura às diferentes autoridades competentes. Em Portugal, a MyCiber já concentra obrigações associadas ao novo Regime Jurídico da Cibersegurança. Ricardo Henriques indica que o Centro Nacional de Cibersegurança está ainda a implementar na plataforma os formulários destinados à notificação de incidentes, que preveem o cruzamento de dados com a Comissão Nacional de Proteção de Dados e a ANACOM.

À medida que aumenta a escala do incidente, cresce também a interação com as autoridades. Para além das notificações obrigatórias, uma organização pode ter de prestar esclarecimentos, fornecer elementos técnicos, atualizar informação anteriormente comunicada ou colaborar na avaliação e acompanhamento do incidente. Para Ricardo Henriques, torna-se então particularmente importante que a informação transmitida seja "rigorosa, consistente e adequadamente validada".

Ainda assim, o sócio da Abreu Advogados considera que a eventual tensão jurídica "concentra-se no conteúdo que se reporta, e não no ato de reportar". Enquanto estiver em causa informação de qualificação e impacto, entende que não existe uma dificuldade significativa. O problema muda quando o detalhe técnico permite que um *threat actor* reconstrua o vetor de ataque. Nesse caso, avança, "o problema deixa de ser de confidencialidade. Passa a ser de segurança da informação".


RICARDO HENRIQUES, ABREU ADVOGADOS

É perante vulnerabilidades ainda por corrigir que este risco se torna mais evidente. O próprio quadro europeu admite que, em determinadas circunstâncias, a divulgação de informação possa ser limitada ou adiada por razões de cibersegurança. Ricardo Henriques dá como exemplo os casos em que "a informação notificada seja, por si só, suficiente para permitir a criação de uma técnica de exploração". Isto é, partilhar informação continua a ser necessário, mas o detalhe divulgado não pode aumentar o risco de exploração da vulnerabilidade.

> O CYBER BLUEPRINT ACRESCENTA "PREVISIBILIDADE À GOVERNAÇÃO DE CRISES, CLARIFICANDO QUEM COORDENA, COMO CIRCULA A INFORMAÇÃO E DE QUE FORMA AS DECISÕES SÃO ESCALADAS"

Ao mesmo tempo, restringir excessivamente a circulação da informação pode comprometer a coordenação. Elsa Lemos identifica precisamente como uma das barreiras a "atribuição de níveis excessivos de confidencialidade a documentos que impede a partilha de dados em tempo útil e prejudica a consciência situacional comum".

O PLANO NÃO CHEGA

Ter um plano de resposta não significa, por si só, estar preparado para uma crise de grande escala. Miguel Gonçalves lembra que uma organização pode ter "políticas, procedimentos, planos de resposta e continuidade muito bem construídos" e descobrir, perante uma situação real, que algumas coisas não funcionam como estavam desenhadas.

É por isso que a preparação passa também por testar esses planos. E não apenas através de exercícios técnicos. Os cenários devem envolver IT, operações, gestão de topo, comunicação, jurídico, proteção de dados, fornecedores e entidades externas, colocando as equipas perante informação incompleta, sistemas indisponíveis, falhas nos canais de comunicação, fornecedores simultaneamente afetados ou decisores inacessíveis. Para Miguel Gonçalves, "um bom exercício não serve para provar que o plano

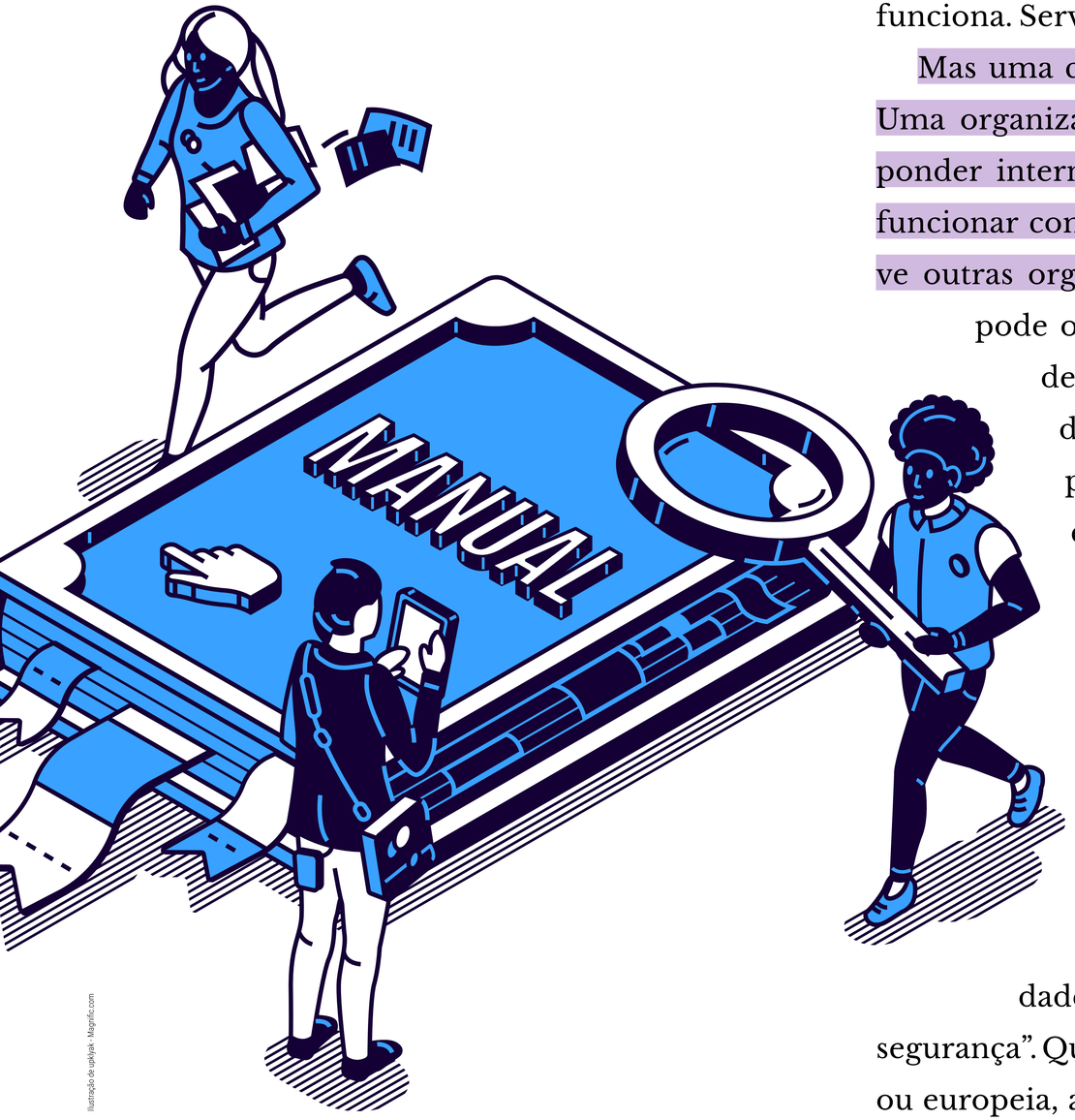


Ilustração de ogklyak - Magnific.com

funciona. Serve para descobrir onde é que ele falha".

Mas uma crise sistémica acrescenta outro teste. Uma organização pode estar preparada para responder internamente e não estar preparada para funcionar como parte de uma resposta que envolve outras organizações, autoridades e países. Isso pode obrigá-la a partilhar informação mais depressa, coordenar decisões com entidades externas e aceitar que as suas prioridades nem sempre coincidem com as do setor ou do país.

Para Miguel Gonçalves, esta mudança exige olhar para além da própria organização e compreender o papel que esta desempenha num ecossistema maior. Na saúde, isso significa reconhecer que "não estamos a proteger *firewalls*, servidores ou redes. Estamos a proteger a capacidade de continuar a prestar cuidados em segurança". Quando a crise ganha dimensão nacional ou europeia, acrescenta, pode ser necessário tomar decisões "pensando no sistema de saúde como um todo, e não apenas na nossa organização".

A preparação tem ainda de considerar as condições em que a organização poderá ser chamada a operar. Elsa Lemos defende que "a organização deve preparar-se para operar num ambiente onde a comunicação é parte da resposta estratégica" e chama a atenção para a "falta de redundância tecnológica" como um fator capaz de agravar uma crise já em curso. Para a especialista, é necessário dispor de canais alternativos de comunicação segura caso as redes normais ou os serviços de Internet fiquem inacessíveis.

Do lado da governação, Ricardo Henriques considera que o *Cyber Blueprint* acrescenta "previsibilidade à governação de crises, clarificando quem coordena, como circula a informação e de que forma as decisões são escaladas". A preparação depende, assim, das equipas, da liderança, dos processos e das relações construídas antes da crise. Como resume Miguel Gonçalves, "numa crise desta dimensão ninguém responde sozinho". ◀



"TUDO DEPENDE DA MATURIDADE DO TÉCNICO E DO DECISOR PARA TER UM CASAMENTO QUE FUNCIONE"

POR MARTA QUARESMA FERREIRA

A EUROTUX DESENVOLVEU A SUA ÁREA DE CIBERSEGURANÇA A PARTIR DA EXPERIÊNCIA ACUMULADA NA RESPOSTA A INCIDENTES. RICARDO OLIVEIRA, CISO DA EMPRESA, ABORDA A EVOLUÇÃO DAS AMEAÇAS, O IMPACTO DA IA E OS DESAFIOS DOS CISO.

Estabelecida há 26 anos, a Eurotux teve a oportunidade de participar em diversos projetos relacionados com *Incident Response* ao longo das mais de duas décadas de atividade. E foi neste âmbito que nasceu a área de cibersegurança da organização portuguesa, numa fase em que o ransomware ainda não existia, mas onde as ameaças eram já uma realidade para os sistemas dos clientes.

Ricardo Oliveira, CISO e Chief Solutions Officer da Eurotux, explica que a empresa teve a oportunidade de experienciar, desde muito cedo, "como é que um atacante ataca", testemunhando as consequências destas ações para as empresas e organismos.

EXPERIÊNCIA COM INCIDENTES MOLDA OFERTA

A experiência adquirida, aliada ao apoio fornecido a diversos episódios de ciberataques – como o do Grupo Impresa, em 2022 –, levou a empresa portuguesa a criar unidades específicas e dedicadas à cibersegurança.

A solução mais conhecida e com uma forte procura é o SOC, com uma monitorização permanente de segurança, 24 horas por dia, que pretende responder às ameaças mais eficazes e cada vez mais sofisticadas, potenciadas também pela Inteligência Artificial (IA).

No portfólio de soluções encontram-se ainda serviços *ad hoc* tradicionais, análise de mobilidades, testes de intrusão e de phishing e serviços de conformidades com normas (ISO 27001, NIS2 e DORA).

REGULAÇÃO CONTRIBUI PARA UMA MAIOR CONSCIENCIALIZAÇÃO

Se, por um lado, os casos dos ciberataques à Vodafone e ao Grupo Impresa geraram um maior *awareness* junto das organizações derivado da sua dimensão e exposição, por outro, a regulação e o maior foco de compliance, com diretivas como a NIS2 e o DORA, levou a que as empresas procu-


RICARDO OLIVEIRA, EUROTUX

“TEMOS CONTROLO SOBRE A TECNOLOGIA, CONTROLO SOBRE O TREINO, CONTROLO SOBRE O QUE É QUE ELA FAZ E COMO É QUE É USADA, PARA NÃO FICARMOS DEPENDENTES DE TERCEIROS”

rassem identificar e compreender como endereçar melhor os riscos.

“Estes eventos marcantes em Portugal e a legislação trouxeram a cibersegurança para a mesa de reuniões das organizações”, refere o responsável.

Ricardo Oliveira aponta ainda para outro fator – o nível técnico. “Até então, a cibersegurança era tipicamente um tema apenas técnico, com muito pouca prioridade, com pouca visibilidade e, essencialmente, era um saco onde se tinha de colocar dinheiro e não se conseguia perceber muito bem o benefício”, frisa.

Na visão do CISO, os requisitos da regulação colocaram a cibersegurança no patamar das administrações e criaram um contexto que implica alterações significativas, não só de orçamentos e equipas, mas, sobretudo, de perceção sobre o nível de risco.

“Tudo depende da maturidade dos dois lados – técnico e decisor –, para em conjunto, ter um casamento que funcione”, reitera Ricardo Oliveira.

INVESTIR DE FORMA INTELIGENTE

Perante o dilema sobre onde as organizações devem concentrar o investimento para melhorar a capacidade de deteção, de resposta e de recuperação, a balança, refere, tende a “pender um bocadinho para a recuperação”.

O responsável considera que a evolução das capacidades de ataque, nomeadamente com o recurso a inteligência artificial, aumenta a possibilidade de um incidente provocar danos significativos nos sistemas das organizações, ainda que não seja possível prever o rumo.

O investimento deve, por isso, abranger mecanismos que permitam à organização retomar a atividade depois de um incidente. “Se eu não investir na recuperação, disaster recovery, testes, cópias de segurança imutáveis e à prova de tudo e mais alguma coisa, pode dar-se o caso de eu ficar sem nada”, alerta.

Com a IA a aumentar as capacidades disponíveis para os atacantes, Ricardo Oliveira defende assim um reforço deste pilar da cibersegurança: "Deve existir uma inclinação para um dos pilares, que é a recuperação, que é o que nos vai salvar no fim do dia".

INTELIGÊNCIA ARTIFICIAL SIM, MAS COM CONTROLO

Para o responsável, a adoção de IA na cibersegurança deve ter como princípio fundamental a soberania tecnológica. Em causa está a dependência de modelos controlados por entidades estrangeiras que pode representar um risco caso o acesso à tecnologia seja limitado ou interrompido por decisões externas.

Ao mesmo tempo, a utilização de IA está a acelerar os ataques. "Há oito, nove meses, os ataques demorariam às vezes semanas; agora demoram horas, às vezes minutos", refere. Esta mudança aumenta a importância da deteção e obriga a reforçar as capacidades defensivas porque, garante Ricardo Oliveira, "se os atacantes têm IA para atacar, então é bom que o pilar da deteção também use IA para ter as capacidades aumentadas, porque senão é uma luta desigual".

A Eurotux optou, por isso, pela utilização de modelos abertos na sua própria infraestrutura, mantendo controlo sobre a tecnologia, o treino e a forma como é utilizada. "Temos controlo sobre a tecnologia, controlo sobre o treino, controlo sobre o que é que ela faz e como é que é usada, para não ficarmos dependentes de terceiros", explica Ricardo Oliveira. Esta abordagem já está também a ser aplicada na defesa da própria organização e dos clientes.

A LINGUAGEM DO NEGÓCIO

Na ótica da proteção contra possíveis ameaças, o CISO defende que as empresas devem procurar cada vez mais estabelecer pontos e solicitar ajuda junto das autoridades nacionais, como é o caso do Centro Nacional de Cibersegurança, através da comunicação de incidentes de segurança, com troca de informação e abertura "para ser ajudado".

Outro dos conselhos implica ganhar maturidade: "Um CISO tem de ter, efetivamente, uma 'costela técnica', isso nunca vai deixar de acontecer, mas deve subir a nível de maturidade para conseguir chegar aos conselhos de administração".

Uma vez aqui chegados, o desafio seguinte passa por conseguir levar a discussão para o nível da gestão, traduzindo conceitos técnicos em risco e impacto para o negócio. Em vez de centrar a conversa nas tecnologias utilizadas, os CISO devem, na visão de Ricardo Oliveira, demonstrar de que forma o investimento permite reduzir a exposição da organização.

No entanto, alerta que o recurso a uma linguagem excessivamente técnica pode revelar-se um entrave na aproximação à gestão. "Se continuarem a falar no EDR, XDR, NDR e afins, vamos continuar no mesmo", alerta.

A mudança exige, assim, maior maturidade por parte dos responsáveis tecnológicos e capacidade para comunicar com quem toma as decisões dentro das organizações. "O meu conselho principal é subir o nível de maturidade para conseguirem conversar com quem os pode ajudar", afirma.

No fim, e uma vez nos conselhos de administração, o intuito é desconstruir o lado técnico da discussão e enquadrar a cibersegurança sempre numa perspetiva de gestão, risco e proteção da própria organização.

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
FOTOGRAFIA: Rui Santos Jorge
COLABORARAM NESTE NÚMERO: Nuno Goes, Nuno Reis, Paulo Martins
DESENVOLVIMENTO WEB: Global Pixel

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

PROPRIEDADES E DIREITOS
A propriedade do título "IT Insight Security" é de MediaNext Lda., uma empresa Jornalística registada da Entidade Reguladora da Comunicação Social com o nº 224011 e NIPC 510 551 866. Proprietários com mais de 5% de Capital Social: Margarida Bento e Pedro Botelho. Todos os direitos reservados. A reprodução do conteúdo (total ou parcial) sem permissão escrita do editor é proibida. O editor fará todos os esforços para que o material mantenha fidelidade ao original, não podendo ser responsabilizado por gralhas ou erros gráficos surgidos. As opiniões expressas em artigos assinados são da inteira responsabilidade dos seus autores.

O IT Insight Security e a MediaNext utilizam as melhores práticas de privacidade sobre dados pessoais e empresariais. Os dados fornecidos para uso exclusivo do serviço de assinantes do IT Insight Security não serão cedidos a qualquer entidade terceira. As informações sobre leitores constantes na base de dados de subscritores do site www.itsecurity.pt estão protegidos pelas melhores práticas de segurança informática.

IT Insight Security é membro de:

ACEPI ASSOCIAÇÃO ECONOMIA DIGITAL

CIWA

Editado por:

media NEXT
STAY AHEAD • STAY RELEVANT