IT Insight SECURITY

#25 AGOSTO 2025

O ESTADO DA NAÇÃO EM CIBERSEGURANÇA

We live and breathe Security

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

Visite: claranet.com/pt/security

claranet | Make modern happen®

COVER

RISK

▼ DECRETO-LEI N.º 22/2025

ANCHOR

▶ HENRIQUE CARREIRO

COVERAGE

▼ PALO ALTO NETWORKS

COVERAGE

▼ C-DAYS 2025

COVERAGE

▼ AWS RE:INFORCE 2025

COVERAGE

▼ KASPERSKY HORIZONS

SECURNET

ALWAYS ONLINE | ALWAYS SECURE

MAIS DO QUE UMA MARCA, UM PARCEIRO DE CONFIANÇA.

☆☆ **HPE 'FY24**	Parceiro do Ano - HPE GreenLake Parceiro do Ano - HPE Aruba Networking
☆ **Veeam Software**	The best COM partner of the year 2024, Portugal
☆☆ **IT Channel Award2025**	Parceiro Cybersecurity Parceiro do Ano

A TECNOLOGIA EVOLUI. E NÓS TAMBÉM.

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

S.LABS

balwurk cyber security

Estado da Nação – "Entre o Alarme e a Ação"

claranet®

O Estado da Nação 2025: Entre a Ilusão da Segurança e a Realidade da Ameaça

CSO chief security officers

Automação na Resposta a Incidentes: Estratégias para Equipas Modernas de Ciberdefesa

EXCLUSIVE NETWORKS

MSSP, Zero Trust e Microsegmentação: o novo tripé da cibersegurança em Portugal

noesis an Altia Company

Cibersegurança em Portugal:
entre o progresso e a urgência de mudança

SECURNET ALWAYS ONLINE | ALWAYS SECURE

Always Smart

VisionWare since 2005

Desinformação e Resiliência Democrática

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.

20 anos

VisionWare

since 2005

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

+100
colaboradores

+200
clientes ativos

5000
projetos desenvolvidos

Os nossos serviços

- Cyber Defense Operations
- Privacy & Legal
- Cybersecurity
- Professional Services
- Ethics & Compliance
- Strategic Intelligence & Risk Analysis
- Forensic Investigations
- VisionWare Academy

Challenging an Unsafe World

Porto | Lisboa | Praia | Mindelo

geral@visionware.pt

+351 225 323 740

SCAN ME

visionware.pt

FAZER O BÁSICO

RUI DAMIÃO

Recentemente, estive numa conferência de cibersegurança e a mensagem passada foi clara: as organizações têm de fazer o básico; não vale a pena pensar muito mais à frente quando as coisas básicas não estão a ser feitas.

Em entrevista com um dos executivos da empresa que organizava essa conferência foi partilhado que a maioria dos ciberincidentes atuais não ocorre devidos a ataques sofisticados, "mas sim por coisas muito básicas".

Segundo dados do Centro Nacional de Cibersegurança, os ciberataques em Portugal aumentaram mais de 716% entre 2015 e o final de 2023 e os cibercriminosos exploram, na maioria das vezes, *passwords* fracas, softwares desatualizados ou definições de segurança mal configuradas.

Na verdade, por vezes, as organizações lançam-se numa corrida tecnológica que, por uma razão ou por outra, é insustentável. Há casos e casos, claro, mas a execução rigorosa de fundamentos básicos oferece, na maioria das vezes, uma proteção eficaz para a maioria das organizações.

Apesar de ter ouvido que 'é preciso fazer o básico', a verdade é que o tema não é novo. Em 2021, numa outra entrevista, um executivo de uma fabricante de cibersegurança dizia que a cibersegurança é "como escovar os dentes três vezes ao dia", onde "é preciso fazer o básico todos os dias".

Ora, de 2021 a 2025 vão quatro anos. No entanto, nestes quatro anos a cibersegurança enfrenta o mesmo problema: fazer o básico.

Há investimentos que têm de ser feitos, claro, mas para a maioria das organizações talvez baste começar pelo básico: gestão de correções e atualizações nos sistemas operativos e nas aplicações; implementação de autenticação multifator; ter *backup* e testar a recuperação; gerir os acessos e os privilégios; e, claro, formar e sensibilizar os colaboradores, que podem – e devem – ser a primeira linha de defesa da organização.

A matemática, na verdade, é simples: implementar estes básicos custa uma fração do que se gasta a recuperar de um incidente. As organizações portuguesas – principalmente as de menor dimensão – têm de começar por aí. ◀

Security Supply Chain

em Conformidade com a SRI2 (NIS2)

Proteja o *Software* contra potenciais ameaças em todas as fases do seu ciclo de vida.

➔ Realizamos uma análise completa da Composição do ***Software (SCA)*** para identificar as componentes de código aberto e as suas potenciais vulnerabilidades.

➔ Geramos o SBOM ***(Software Bill of Materials)***, oferecendo transparência e rastreabilidade de cada elemento do software

➔ A nossa abordagem estende-se à análise da **cadeia de fornecimento de software,** identificando e mitigando os riscos associados a componentes de terceiros.

mail@balwurk.com

balwurk cyber security

HENRIQUE CARREIRO

A SENTINELA PROATIVA

O tema unificador da cibersegurança tem sido, por demasiado tempo, sobretudo uma narrativa de contenção. Descreve-se uma luta assimétrica, uma defesa entrincheirada, reagindo a ameaças num perímetro digital cada vez mais poroso. É a doutrina do muro, do fosso e do alarme — uma estratégia que, embora necessária, consome recursos vastíssimos e coloca o defensor num estado de perpétua desvantagem. Perante este cenário, uma questão fundamental impõe-se: e se o paradigma defensivo estiver, na sua génese, incompleto? E se à contenção se pudesse sobrepor a antecipação?

Um desvio conceptual significativo começa a tomar forma, materializado em projetos que redefinem a própria natureza da defesa. O mais notável é talvez o Big Sleep, desenvolvido em colaboração pela DeepMind e pelo Project Zero da Google, um agente de Inteligência Artificial que personifica esta nova filosofia. Não se trata de um vigilante passivo, mas de um caçador digital, um sentinela proativo. A sua função não é esperar por um ataque, mas procurar ativamente as fragilidades que o poderiam permitir. A sua recente descoberta de uma vulnerabilidade em SQLite (CVE-2025-6965), antecipando a sua exploração por atores hostis, não é apenas uma vitória técnica. É a prova de conceito de que é possível virar o tabuleiro do jogo e impor um novo ritmo ao adversário. E esta não é uma descoberta de somenos importância. O SQLite é uma ferramenta silenciosa, mas usada

A QUESTÃO CRÍTICA QUE SE NOS COLOCA JÁ NÃO É SE CONSEGUIMOS CONSTRUIR ESTES NOVOS GUARDIÕES, MAS SE TEREMOS A MATURIDADE E A SABEDORIA PARA OS INTEGRAR DE FORMA SEGURA E EFICAZ NA NOSSA SOCIEDADE DIGITAL

por milhões de utilizadores, e omnipresente, por exemplo, nas aplicações para smartphones. O seu código, produzido por um grupo restrito de colaboradores e sujeito a um dos mais intensivos escrutínios do mundo do software, parecia uma fortaleza quase inexpugnável. Que tenha sido um agente a descobrir uma vulnerabilidade perante tais circunstâncias, é um sinal inequívoco do potencial transformador da segurança assente em agentes.

O corolário direto desta evolução é uma revalorização do analista humano, impulsionada pela introdução de agentes de IA em plataformas como o Timesketch — uma ferramenta de código aberto também desenvolvida pela Google que promete automatizar o trabalho de análise forense mais exaustivo. Delega-se à máquina a análise de força bruta sobre volumes de dados massivos, o "ruído" constante da atividade digital, libertando a cognição humana para a tarefa em que é insubstituível: a dedução estratégica, a interpretação de contextos subtis e a intuição. Assiste-se, assim, a uma transição do analista-operário, afogado em alertas, para o analista-estratega, cuja atenção se foca exclusivamente no "sinal" de uma ameaça complexa. A IA torna-se um amplificador da inteligência humana.

Seria, contudo, uma ingenuidade celebrar este avanço sem um profundo sentido de responsabilidade. A potência destas ferramentas exige um ecossistema de governação robusto e transparente, onde a sua autonomia seja balizada por princípios de *secure-by-design* e por uma supervisão humana inequívoca. Este ecossistema, por sua vez, edifica-se sobre o alicerce da colaboração entre a indústria, a academia e o setor público. Iniciativas como a **Coalition for Secure AI** (CoSAI) são a prova deste movimento, e a decisão da Google em ceder dados do seu **Secure AI Framework** (SAIF) para acelerar o trabalho do consórcio é um exemplo tangível do seu potencial. Este esforço conjunto não é um mero apêndice, mas a condição *sine qua non* para gerar a confiança sobre a qual esta nova era de segurança deve assentar.

Em última análise, o que testemunhamos é a passagem de uma cibersegurança de reação para uma de antecipação. Estamos a dotar o nosso ecossistema digital não apenas de escudos mais resistentes, mas de um sistema imunitário inteligente e preditivo. A questão crítica que se nos coloca já não é se conseguimos construir estes novos guardiões, mas se teremos a maturidade e a sabedoria para os integrar de forma segura e eficaz na nossa sociedade digital. ◀

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

CONSELHO DE MINISTROS APROVA NOVO REGIME DE CIBERSEGURANÇA

O Conselho de Ministros aprovou a proposta de lei – que ainda irá passar pela Assembleia da República – que regula o novo regime jurídico de cibersegurança.

"Se é verdade que Portugal não tem no seu espaço físico uma situação de guerra ou de conflitos e agressões ao país e ao Estado, o mesmo não é verdade para o seu ciberespaço", começou por dizer António Leitão Amaro, ministro da Presidência do XXV Governo Constitucional da República Portuguesa na conferência de imprensa onde foi anunciada a aprovação do novo regime de cibersegurança no âmbito da transposição da diretiva europeia NIS2 por parte do conselho de ministros.

A proposta de lei terá de ser discutida e votada na Assembleia da República e procura criar uma estrutura de riscos proporcional à dimensão e características dos serviços que as entidades prestam. O governo olhou para a diretiva NIS2 e optou "por um regime de uma matriz de risco em função da dimensão e do nível e criticidade das empresas s instituições". ◀

NATO APROVA CIBERSEGURANÇA COMO GASTOS DE DEFESA

Membros da Aliança Atlântica aprovaram um investimento de 5% do PIB em Defesa. Desta percentagem, 1,5% estão alocados a despesas indiretas onde se inclui a cibersegurança

Os aliados da NATO chegaram a acordo para aumentar os gastos com defesa, investindo 5% do PIB até 2035, com revisão dos objetivos em 2029. Destes 5%, 3,5% são destinados à defesa direta e os restantes 1,5% a despesas indiretas com defesa, incluindo cibersegurança.

"A segurança já não pode ser pensada apenas nos domínios tradicionais do ar, do mar e da terra, mas também na tecnologia, na cibernética e na força da nossa sociedade democrática", defendeu Mark Rutte, Secretário Geral da NATO, na abertura da cimeira, em Haia, nos Países Baixos.

Algumas das despesas com o ciberespaço deverão estar abrangidas na fatia dos 3,5% e deverão incluir orçamentos para comandos cibernéticos militares e proteções para redes militares operacionais. ◀

EXCLUSIVE NETWORKS

INNOVATE TOGETHER

Promoting collaborative innovation in cybersecurity

ARISTA · BITSIGHT · Cymulate · druva · Extreme networks · Gigamon · HYCU · imperva a Thales company

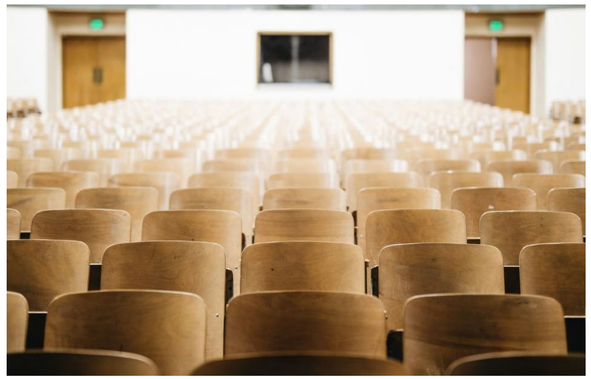
infoblox · netskope · NOZOMI NETWORKS · ONE IDENTITY · paloalto NETWORKS · proofpoint · rubrik · SentinelOne

tenable · THALES · tufin · wasabi · ZERO. Networks

www.exclusive-networks.com/pt

CIIWA REALIZA TERCEIRA EDIÇÃO DE CURSO DEDICADO A NIS2 E DORA

No quadro de uma parceria entre a CIIWA, a Cuatrecasas e a Cybers3c, a terceira edição do curso NIS2 e DORA – o caminho da implementação e do compliance acontece a partir de 10 de setembro.



Após o sucesso da segunda edição, a CIIWA anunciou a realização da terceira edição do curso NIS2 e DORA – o caminho da implementação e do compliance. No quadro de uma parceria com a Cuatrecasas e Cybers3c, esta oferta formativa destaca-se pela abordagem prática sobre os novos requisitos regulatórios europeus em matéria de cibersegurança e resiliência digital operacional. A sessão de abertura tem lugar no dia 10 de setembro de 2025.

Com um total de 30 horas, as aulas decorrem em regime pós-laboral, segundo um modelo híbrido. As propinas têm um valor de 850 euros, ou 650 para associados da CIIWA. As entidades não associadas que inscreverem duas ou mais pessoas no curso têm direito a 10% de desconto no terceiro inscrito e seguintes. *As inscrições já estão abertas*.

CENTRO NACIONAL DE CIBERSEGURANÇA LANÇA ALERTAS DE MALWARE E DE VULNERABILIDADE

O CNCS lançou recentemente dois alertas – um de malware e outro de vulnerabilidade – referente ao BadBox e ao Linux.

O Centro Nacional de Cibersegurança lançou recentemente dois alertas – um de vulnerabilidade e outro de malware – que dizem respeito ao Linux e ao BadBox2.0.

O alerta de vulnerabilidade referente ao Linux é uma vulnerabilidade crítica que afeta as versões Sudo entre 1.9.14 e 1.9.17, inclusive. Esta vulnerabilidade permite que um atacante local escale os seus privilégios, podendo executar comandos arbitrários como root.

O Centro Nacional de Cibersegurança também lançou um alerta para o malware BadBox. Esta é "uma ameaça sofisticada que compromete dispositivos Android, incluindo Smart TV, aparelhos de *streaming*, tablets e projetores digitais. Identificado inicialmente em 2023, o BadBox é frequentemente pré-instalado em dispositivos de baixo custo, maioritariamente fabricados na China, através de ataques à supply chain ou por intenção dos fabricantes".

noesis
an Altia Company

DARKTRACE

Detete todas as ciberameaças à sua empresa em apenas 4 semanas

Peça a sua avaliação gratuita
de Darktrace Enterprise Immune System

- 4 Semanas de utilização de solução de Cyber AI, sem custos
- Proteção dos colaboradores e organização contra ameaças de segurança
- Ação imediata sobre qualquer ameaça ou vulnerabilidade
- Tecnologia líder mundial assente em Machine Learning

Saiba mais

Helping your business **grow faster**

Portugal · Espanha · Irlanda · Holanda · Brasil · EUA

www.noesis.pt

PORTUGAL ENTRE OS PAÍSES EUROPEUS COM MAIOR PERCENTAGEM DE ATAQUES DE MALWARE EM PC

No primeiro trimestre de 2025, 8,7% dos utilizadores de PC em Portugal foram alvo de malware, colocando o país acima da média global e entre os mais afetados da Europa.

O mais recente estudo da Kaspersky, *IT Threat Evolution in Q1 2025: Non-Mobile Statistics*, revela que 8,70% dos utilizadores de PC em Portugal foram alvo de ataques de malware no primeiro trimestre de 2025, um valor superior à média global de 6,46%.

Para avaliar o risco de infeção online, os especialistas da empresa de cibersegurança calcularam a percentagem de utilizadores Kaspersky cujos computadores ativaram o antivírus web durante o período em análise. Estes dados refletem o nível de agressividade do ambiente digital em que os equipamentos operam, variando significativamente consoante a região.

Portugal surge na 12.ª posição a nível mundial, imediatamente atrás do Peru (8,78%) e à frente do Nepal (8,38%).

CLOUDFLARE LANÇA FUNÇÃO QUE BLOQUEIA RASTREADORES DE IA POR PADRÃO

A Cloudflare começou a bloquear, por padrão, o acesso de bots de inteligência artificial aos sites que protege, exigindo consentimento explícito dos proprietários.

A Cloudflare anunciou uma alteração estrutural na forma como os rastreadores de Inteligência Artificial (IA) acedem a conteúdos online. A partir de agora, o acesso por parte de bots de IA passa a ser bloqueado por padrão em todos os websites geridos pela empresa, sendo apenas autorizado mediante consentimento explícito dos proprietários.

Esta decisão surge num momento de crescente debate em torno da recolha de dados online para o treino de modelos de linguagem de grande escala (LLM), como o ChatGPT, Llama ou Grok. A prática de scraping, que consiste em recolher conteúdo da web para alimentar estes modelos, tem levantado preocupações sobre direitos de autor, privacidade e sustentabilidade económica da internet.

09 OUT 2025 | LISBOA

A VOZ DOS CISO

A quarta edição da IT Security Conference 2025 já tem data marcada para **09 de outubro, em Lisboa**, onde os temas mais relevantes sobre o ecossistema da cibersegurança voltam a estar em debate e análise pelos mais proeminentes especialistas da área.

MARQUE A DATA NA SUA AGENDA.

PARCEIROS:

Diamond

EM BREVE

Platinum

ACS Agile Cybersecurity Solutions · CHECK POINT · elred · claranet · FORTINET · HPE aruba networking · pwc · SOPHOS

Golden

FUJIFILM · hp · Ingecom IGNITION An Exclusive Networks Company · LOGICALIS Architects of Change · ManageEngine · redShift · SECURNET ALWAYS ONLINE | ALWAYS SECURE · VARONIS

Silver

ART RESILIA · balwurk cyber security · cisco · devoteam Cyber Trust · DIVULTEC · IDW YOUR BUSINESS · OUR CHALLENGE · kaspersky · oramix EXPERT SERVICES · TD SYNNEX · VisionWare since 2005 · V-Valley

Bronze

WatchGuard · eset Digital Security Progress. Protected.

Institutional Partners

CNCS Centro Nacional de Cibersegurança PORTUGAL · CIWA

SOC COM IA: O PRÓXIMO PASSO NA CIBERSEGURANÇA

A PRÓXIMA GERAÇÃO DOS SECURITY OPERATIONS CENTERS (SOC) ESTÁ A NASCER DA ALIANÇA ENTRE INTELIGÊNCIA ARTIFICIAL, AUTOMAÇÃO E KNOW-HOW HUMANO — E ESSE FOI O MOTE DE UM ENCONTRO EXCLUSIVO QUE JUNTOU PALO ALTO NETWORKS, IBM E LÍDERES DE CIBERSEGURANÇA NACIONAIS PARA DEBATER O FUTURO DA PROTEÇÃO DIGITAL. O EVENTO MOSTROU POR QUE RAZÃO É URGENTE REPENSAR OS SOC PARA ENFRENTAR AMEAÇAS MAIS RÁPIDAS E SOFISTICADAS.

A transformação dos *Security Operations Centers* (SOC) com Inteligência Artificial (IA) reuniu líderes da IBM, Palo Alto Networks e um grupo exclusivo de profissionais de cibersegurança para explorar como a IA está a revolucionar os SOC. Entre casos reais, debates estratégicos e as últimas inovações, este evento exclusivo lançou luz sobre o futuro da segurança digital e mostrou como a combinação entre tecnologia avançada e experiência humana está a transformar a forma como as organizações respondem a ameaças cada vez mais complexas e rápidas.

O encontro procurou evidenciar, como referiu **Luís Lança, Country Manager da Palo Alto Networks**, como a combinação entre tecnologia e serviços permite construir SOC mais eficazes, recorrendo a análises comportamentais para acelerar a deteção e a resposta a incidentes. Essa visão foi claramente partilhada pela IBM, que, ao distinguir o papel da IBM Technology e da IBM Consulting, fez questão de sublinhar – nas palavras de **Carlos Creus, Security Services Leader da IBM –** que o setor tec-

À ESQUERDA CARLOS CREUS,SECURITY SERVICES LEADER DA IBM, À DIREITA LUÍS LANÇA, COUNTRY MANAGER DA PALO ALTO NETWORKS

PEDRO FRANCISCO, CORTEX REGIONAL SALES MANAGER DA PALO ALTO NETWORKS

CHRISTIAM CARRILLO, CYBER THREATS MANAGEMENT OFFERING LEADER DA IBM

nológico da empresa "continua a vender software, dados e infraestrutura, e mantém as suas redes de parceiros". Realçou ainda que a aliança apresentada no evento não surge apenas "por um interesse inicial, mas porque ambas as empresas têm uma visão muito semelhante sobre para onde vamos e os desafios que enfrentamos".

"Até dezembro do ano passado, os atacantes demoravam cerca de um dia entre a penetração e o impacto real. Agora, 20% dos cenários acontecem em apenas algumas horas. Isto obriga-nos a repensar os modelos operacionais para nos adaptarmos a esta nova realidade", disse **Pedro Francisco, Cortex Regional Sales Manager da Palo Alto Networks**, numa apresentação onde deu conta da urgência da transformação dos SOC face à crescente complexidade e velocidade dos ataques. Sublinhou ainda o papel central da plataforma XSIAM na automatização e na redução dos falsos positivos, o que permite às equipas de segurança focar-se em ações proativas e decisivas.

Christiam Carrillo, Cyber Threats Management Offering Leader da IBM, destacou a forma como a empresa está a apoiar a transformação dos SOC, sublinhando o papel da inteligência artificial e da automação para tornar os serviços mais proativos e eficientes. "O nosso objetivo mínimo é automatizar pelo menos 55% de todo o processo de gestão de alertas, desde a deteção à investigação e resposta, integrando tudo com as tecnologias que o cliente já possui", afirmou. Christian Carrillo referiu ainda que esta evolução é indispensável para enfrentar o aumento do volume de dados e a complexidade tecnológica, defendendo que "há alguns anos, esta tecnologia não existia; hoje, é o impulsionador que permite libertar as equipas humanas para atividades de maior valor".


RAQUEL LOPEZ, SECURITY SERVICES SOLUTION DESIGN & PROJECTS LEADER DA IBM


PAULO MARTINS, DIRETOR IT & OPERAÇÕES DO SPORT LISBOA E BENFICA

Para destacar o valor de um projeto bem estruturado, **Raquel Lopez, Security Services Solution Design & Projects Leader da IBM**, trouxe um caso de sucesso de como a empresa conseguiu transformar o SOC de um cliente do setor financeiro em Espanha, através de uma transição sem sobressaltos. "Obtivemos zero incidências durante todo o projeto, o cliente felicitou-nos e melhorámos consideravelmente as capacidades de deteção e resposta", afirmou. Sublinhou ainda que o êxito se deveu à combinação entre experiência, planeamento detalhado, envolvimento antecipado dos vários *stakeholders* e uma estratégia personalizada, que permitiu avançar sem qualquer interrupção nos sistemas já existentes.

Paulo Martins, Diretor IT & Operações do Sport Lisboa e Benfica: "Estou inclinado a acreditar que não só o SOC, mas as operações das organizações vão mudar. Falou-se muito da complexidade tecnológica dentro das organizações, que hoje é grande, e da falta de *know-how*, e acho que todos sofremos um pouco com isso. Não falando só do SOC, mas de uma estratégia mais global, estou alinhado com esta visão e temos vindo a trabalhar nela, usando IA e criando processos mais integrados. Agora, vai haver uma fase de transição em que as empresas vão começar a utilizar IA autónoma. Temos feito esse caminho, muito focados em ferramentas que nos criam *playbooks* automáticos na área de operações, seja para o SOC, seja fora do SOC. Penso que daqui a dois anos, com a grande aceleração da IA, isso vai apoiar não só o SOC, mas todas as operações da organização, mudando funções, pessoas e competências"

David Marques, Head of Cybersecurity do Grupo Nabeiro: "A automação é, evidentemente, um dos objetivos que vemos aqui claramente, especialmente para melhorar algo que, para mim, é fundamental em termos de SOC e resposta a incidentes: a rapidez de resposta. Trabalhei muitos anos do lado do


DAVID MARQUES, HEAD OF CYBERSECURITY DO GRUPO NABEIRO


LUÍS LANÇA, COUNTRY MANAGER DA PALO ALTO NETWORKS


CARLOS CREUS, SECURITY SERVICES LEADER DA IBM

prestador de serviços e fiz muita resposta a incidentes no passado, e uma das lições mais claras é que, na grande maioria das vezes, quando os incidentes acontecem, os dados estão todos lá. Não houve foi tempo de olhar para eles e responder de forma mais efetiva. Portanto, a automação penso que nos pode dar esta diminuição do tempo de resposta, que hoje em dia é fundamental. Esse, claramente, é um caminho que estamos a seguir e penso que é inevitável. Por outro lado, um dos desafios é sempre o custo versus benefício de colocar mais fontes de dados, mais alarmística"

Luís Lança, Palo Alto Networks: "Uma das previsões para 2025 é exatamente que, em 2030, mais de 70% dos SOC vão estar automatizados. A principal vantagem que vemos hoje é criar um primeiro passo, que é a visibilidade. Eu tenho os meus dados, mas a visibilidade sobre eles não existe; portanto, se não a tenho, não consigo melhorar o meu tempo de resposta. Vejo isto como uma plataforma modular, que consolida alguns dados, mas que depois precisa de ser automatizada e de ter contexto de negócio, para poder ajudar a decidir melhor. E, tanto numa vertente de *threat hunting* como numa vertente de *reactive service*, fizemos assim para deteção e resposta"

Carlos Creus, IBM: "Estamos a gerar assistentes de gestão do conhecimento. O que quero dizer com gestão do conhecimento? O modelo RAC, onde fazem casos, não é só a documentação, mas também guardar como foi resolvido, qual era a causa, com quem se consultou, qual é a informação do negócio ao redor deste incidente, e guardar isso. Guardam esse conhecimento que as equipas depois podem consultar e usar como parte da sua ferramenta no dia

a dia. Não só estamos a potenciar, como estamos a capitalizar, porque se houver qualquer rotação nessas equipas, o sistema de gestão do conhecimento mantém-se dentro da empresa"

Sérgio Trindade, IT Director of Solutions and Digital Systems, CISO, Águas do Tejo Atlântico: "Estamos a competir com modelos de IA, ferramentas avançadas. O ataque já não é como o identificávamos anteriormente. Estamos a tentar fazer o que podemos internamente, com recursos humanos que não existem no mercado, porque os que existem ou não estão bem preparados ou os que estão, em geral, não temos budget para pagar. Vamos tentando fabricar o que podemos. Nesse "fabricar o que podemos" para construir um SOC, tentamos aliar ferramentas diferentes que não falam entre si. E isso foi exatamente o que retive do que poderíamos ter em soluções deste género: entre fabricantes, distribuidores, consultores, começar a fazer aquilo que já vimos acontecer noutro tipo de guerras"


SÉRGIO TRINDADE, IT DIRECTOR OF SOLUTIONS AND DIGITAL SYSTEMS, CISO, ÁGUAS DO TEJO ATLÂNTICO


NUNO PALMA, DIRETOR DO DEPARTAMENTO DE TECNOLOGIAS DE INFORMAÇÃO DA CÂMARA DE CASCAIS

Nuno Palma, Diretor do Departamento de Tecnologias de Informação da Câmara de Cascais: "Na administração pública, acho que, para além do mais, a componente do planeamento estratégico e, sobretudo, do conhecimento dos *stakeholders* é muito crítico. Se esta tecnologia não for assimilada e, em termos de aprendizagem automática, não tivermos regras que sejam efetivamente alimentadas, modelos construídos com base na experiência de cada um, dificilmente a administração pública estará, hoje ou amanhã, preparada para qualquer ataque. Enquanto não pensarmos em conjunto e não definirmos uma estratégia com a ajuda das entidades especializadas – que são as que nos podem ajudar diretamente – dificilmente esta automatização será rentabilizada positivamente"

Jorge Moreira, Information Security Officer da Universidade do Porto: "Na realidade, temos de ter espírito crítico, principalmente com a IA. São coisas

JORGE MOREIRA, INFORMATION SECURITY OFFICER DA UNIVERSIDADE DO PORTO

PAULO FERREIRA, ESPECIALISTA DSST, IGFEJ

ALBERTO BRUNO, HEAD OF SOC DA ALTICE PORTUGAL

que temos de questionar: como é que vamos fazer a arquitetura das coisas? Porquê? É nesta vertente que as equipas internas têm de trabalhar. Se perdemos demasiado tempo a olhar para o incidente, não temos tempo sequer para questionar. Isto funciona, a nível geral, porque as pessoas não se questionam. Acomodam-se às situações, tomam as coisas como garantidas e não avançam para o próximo passo. Na área da cibersegurança, temos de ser capazes de questionar"

Paulo Ferreira, Especialista DSST, IGFEJ: "É necessário que as equipas consigam responder melhor a esse fluxo, tendo em conta os ataques que vão surgindo, e é óbvio que não podemos fugir disso. A inteligência artificial representa uma viragem e, queiramos ou não, não vamos escapar a este novo desafio. A própria IA vai acabar por ajudar a gerir todo esse fluxo enorme, que hoje começa a ser complicado, e permitirá responder de forma mais eficaz. Contudo, é importante frisar que a IA não irá substituir as estratégias das organizações, públicas ou privadas, e será difícil encontrar uma organização que não inclua soluções de IA nas suas estratégias. No que diz respeito à cibersegurança, devemos olhar para a IA como um suporte"

Alberto Bruno, Head of SOC da Altice Portugal: "Quando automatizamos e deixamos a máquina fazer a triagem de primeiro nível, ou até um pouco mais, e tomar decisões sobre como mitigar, temos de ter total certeza de que isso não vai prejudicar a operação. Naturalmente, quem ataca pode usar a IA como quiser: se falhar, tenta outra vez, sem problema. Quem está a defender através de automação ou inteligência artificial, se falhar, tem um problema grave. Temos de ter confiança total nestas tecnologias e garantir que os resultados são os esperados. Depois, há obviamente a questão dos custos: quanto é que esta mudança nos vai custar e quanto é que vai render – no fundo, o tal custo-benefício"

José Augusto Silva, Head of Information Security Unit da Universidade do Porto: "Sou adepto do modelo híbrido através do apoio de um parceiro que nos apoie. Nós não temos um SOC 24/7, por isso a resiliência passa por aumentar essa cobertura. Depois, há a heterogeneidade das fontes e dos sistemas, que é outro problema, assim como o turnover do talento – e este não é um problema exclusivo do setor público, também acontece no privado. Ao adotarmos um modelo híbrido e utilizarmos um tipo de automação, vamos conseguir reter e atrair recursos que queiram usar soluções inovadoras, porque não é só o salário que mantém os membros de uma equipa"

Pedro Galveias, Leading Cybersecurity Operations da TAP Air Portugal: "Estamos a tentar ganhar alguma visibilidade, sobretudo mais contexto na nossa operação. Sou adepto desta abordagem híbrida, principalmente numa empresa que tem um setor muito específico, em que o contexto é fundamental. Um dos nossos maiores objetivos no fim desta jornada é conseguir traduzir a existência, ou não, de uma deteção, que pode ter um custo consoante o ativo. No final do dia, poder traduzir o que estamos a fazer em euros, que são salvos todos os dias, fará uma enorme diferença no desenvolvimento da própria empresa"

Vítor Almeida, Cybersecurity, SPMS: "A capacidade de termos um SOC que responda de forma rápida e assertiva a determinados incidentes é muito importante. A automação vai ajudar bastante as equipas. Relativamente à estratégia da minha empresa, estamos a falar de vidas humanas, o que torna tudo ainda mais sensível. Por isso, há um investimento


FERNANDO AGUIAR, CYBERSECURITY OPERATIONS E SOC MANAGER DO BANCO CTT


DUARTE FREITAS, IBM CONSULTING - CYBERSECURITY SERVICES

crescente para garantir que os componentes mais complexos de IT possam ser monitorizados e que as equipas possam intervir com maior rapidez face a possíveis incidentes"

Fernando Aguiar, Cybersecurity Operations e SOC Manager do Banco CTT: "Para planear uma mudança ao nível da cibersegurança, é fundamental começar pelo início: olhar para os desafios que existem e dar-lhes resposta. De forma geral, passam pelo ambiente com diversas plataformas, os alertas que surgem de todos os lados e a dificuldade em centralizá-los, de modo a proporcionar à equipa a visibilidade necessária para responder eficazmente. O conceito de plataformização chama a atenção e traz algum alívio, sobretudo se estivermos a falar de uma plataformização que não nos prenda a um único fabricante – ou seja, que permita reunir todas as soluções numa só plataforma, de forma holística, com visibilidade mais assertiva para as operações"

Duarte Freitas, IBM Consulting - Cybersecurity Services: "Relativamente à retenção de talento, é importante não só a componente salarial, mas também a forma como tratamos as pessoas. O trabalho de nível 1, por exemplo, o que um *security analyst* tem de fazer, é muito repetitivo. É uma carreira e muitos chegam com ambições de progredir no plano de carreira em cibersegurança, mas as tarefas são bastante repetitivas. Acredito que a automação e a introdução de técnicas de IA podem ter um impacto muito positivo, pois vão transferir essas pessoas para tarefas de maior valor, libertando-as do dia a dia monótono e repetitivo" ◀

ESTADO DA NAÇÃO: ONDE ESTÁ A CIBERSEGURANÇA EM PORTUGAL?

POR RUI DAMIÃO

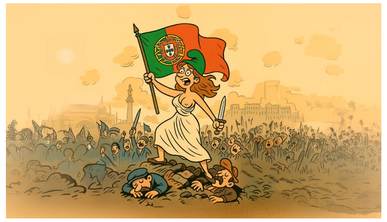
REGULAMENTAÇÃO, NOVAS TECNOLOGIAS E ESCASSEZ DE TALENTO CONTINUAM A MARCAR O PANORAMA DE CIBERSEGURANÇA NACIONAL, QUE TRAZEM OPORTUNIDADES, MAS TAMBÉM DESAFIOS PARA AS ORGANIZAÇÕES PORTUGUESAS. BALWURK, CLARANET PORTUGAL, EXCLUSIVE NETWORKS, NOESIS, SECURNET E VISIONWARE PARTILHAM A SUA VISÃO SOBRE COMO ESTÁ A CIBERSEGURANÇA EM PORTUGAL. BEM-VINDOS AO ESTADO DA NAÇÃO.

Já não há dúvidas: a cibersegurança é uma necessidade de todas as organizações. É preciso olhar para as tecnologias, para os processos e, também, para as pessoas para proteger as organizações numa altura em que os negócios são cada vez mais digitais.

No meio de regulamentação – como a NIS2 e a DORA – ou de tecnologias que chegam cada vez a mais organizações – como a Inteligência Artificial (IA) –, as organizações têm de se adaptar a um cenário de ameaças mais complexo para estarem seguras.

Para uma audiência de mais de 350 leitores, a IT Security organizou uma vez mais – pelo quarto ano consecutivo – o Estado da Nação em Cibersegurança, onde os representantes de seis empresas portuguesas partilharam a sua visão sobre como está a cibersegurança em 2025.

PARA VER O VÍDEO CLIQUE SOBRE A IMAGEM



COMO É QUE AVALIAM A MATURIDADE DAS ORGANIZAÇÕES PORTUGUESAS EM CIBERSEGURANÇA COMPARATIVAMENTE A OUTROS MERCADOS EUROPEUS?

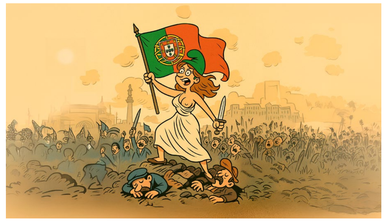
Bruno Castro, Founder & CEO, VisionWare: "Antes o investimento em cibersegurança era bizarro; tínhamos de explicar que investir em cibersegurança não era um custo. Hoje já não vejo as coisas assim. É difícil encontrar um gestor de uma empresa que não perceba a importância de investir em cibersegurança e não saiba a sua posição de risco. Sobre o mercado nacional, tivemos os últimos cinco, seis anos em que o cibercrime teve muito impacto no negócio, que se tem tornado cada vez mais digital. A cibersegurança deixou de ser vista um custo e passou a ser um investimento"

David Grave, Security Director, Claranet Portugal: "Temos do melhor que se faz na Europa e no mundo em grandes empresas portuguesas, com uma estratégia de passar 'debaixo do radar'. São organizações que estão muito seguras e já passaram a realidade de comprar as caixinhas de segurança. Mas isto é 2% do tecido empresarial. Devemos olhar para o que fazem, mas preocupa-me o que fazem as outras 98%. Acredito que exista um número considerável de organizações em que cibersegurança é comprar um antivírus ou uma firewall e nem exista o conceito de governança. Temos, claramente, dois mundos muito diferentes no país"

Elizabeth Alves, Sales Director, Exclusive Networks: "O Global Security Index 2024 posiciona Portugal entre os países mais desenvolvidos nesta matéria. Isto deve-se às políticas que temos e, também, pela capacitação que tem evoluído muito nos últimos anos. Aquilo que vemos é um crescimento de maturidade por parte das empresas nesta matéria. Hoje, encontramos organizações que têm um departamento que só leva a área de cibersegurança. No entanto, temos muitas pequenas e médias empresas. Há maturidade, mas falta a capacidade de implementação à escala certa"

BRUNO CASTRO, FOUNDER & CEO, VISIONWARE

"É DIFÍCIL ENCONTRAR UM GESTOR DE UMA EMPRESA QUE NÃO PERCEBA A IMPORTÂNCIA DE INVESTIR EM CIBERSEGURANÇA E NÃO SAIBA A SUA POSIÇÃO DE RISCO"



MIGUEL AZEVEDO, IT OPERATIONS, CLOUD & SECURITY SENIOR MANAGER, NOESIS

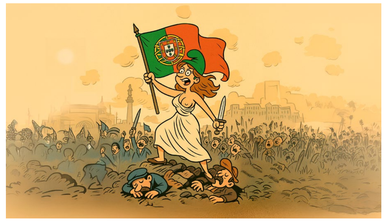
"É IMPORTANTE A ORGANIZAÇÃO TER A VISIBILIDADE DOS GAPS QUE TEM DENTRO DA SUA INFRAESTRUTURA E FAZER SEMPRE UM PLANEAMENTO PORQUE O INVESTIMENTO PODE SER CURTO A DOIS OU TRÊS ANOS PARA TER UM CAMINHO"

Miguel Azevedo, IT Operations, Cloud & Security Senior Manager, Noesis: "Da nossa experiência em vários mercados, o nível de maturidade nas organizações que têm uma forte dependência do IT é tendencialmente mais elevado. Aquelas que não têm tanto essa dependência, ou até aquelas que não têm um grande impacto das regulamentações, acabam por ter um nível de maturidade mais baixo em cibersegurança"

QUAL É O MAIOR *GAP* ENTRE AS NECESSIDADES REAIS DAS ORGANIZAÇÕES PORTUGUESAS E AS SOLUÇÕES QUE O MERCADO ESTÁ A OFERECER?

Ricardo Rodrigues, CEO, Balwurk: "Há uma utilização excessiva da tecnologia e não tanto da cibersegurança aplicada ao negócio. Na gestão de topo existe uma maior maturidade em cibersegurança, mas não nos podemos esquecer que os principais interlocutores não são a gestão de topo. Passamos ainda pelo CISO – que pode ainda não fazer parte do *board* – e verifica-se, ainda, um *gap* entre os serviços orientados para o contexto do negócio para a tecnologia que o mercado oferece, mesmo sabendo que os produtos em si são necessários"

Elizabeth Alves, Exclusive Networks: "O maior desfasamento está na forma como a oferta se ajusta à necessidade e operacional das empresas. Vemos empresas a procurar soluções robustas e completas – soluções *premium* –, mas não querem pagar o valor que elas custam, até porque, por vezes, não têm esse orçamento. O grande tecido empresarial que temos deve estar apoiado, tentar perceber e entender o que é que tem impacto em termos de segurança para a continuidade do negócio da organização. Muitas vezes, as empresas não têm estrutura para realizar isso e precisam de apoio"

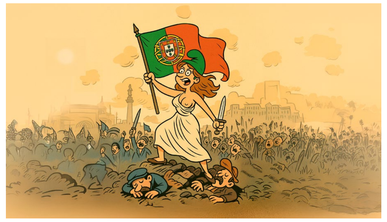


Bruno Castro, VisionWare: "Desenhamos as melhores soluções para cada risco em cima da mesa. Tentamos perceber qual é o modelo de negócio do cliente e damos conselhos nesse sentido. As empresas não devem cair na tentação da vacina mágica que é vendida pelos fabricantes e devem avaliar muito bem que aquilo que têm dentro de portas é suficiente ou não para o seu modelo de negócio. Há uma oferta como nunca houve antes, mas grande parte disto é caro e difícil de manter"

COM OS ORÇAMENTOS DE CIBERSEGURANÇA SOB PRESSÃO, QUE INVESTIMENTOS CONSIDERAM ABSOLUTAMENTE CRÍTICOS EM COMPARAÇÃO COM UM *NICE TO HAVE*?

Miguel Barreiros, Sales & Marketing Director, Securnet: "Se queremos fazer um bom trabalho, temos de fazer de filtro entre aquilo que são os interesses dos fabricantes e as necessidades das empresas. Os investimentos dependem sempre da realidade das organizações. Não há caixas mágicas, de facto. O que podemos dar como conselho aos investimentos sob pressão – e são sempre todos – é começar a conhecerem-se a si próprios. As organizações precisam de conhecer aquilo que têm para poderem agir. Muitas vezes começam a agir sem saber sobre o quê"

Miguel Azevedo, Noesis: "É importante a organização ter a visibilidade dos *gaps* que tem dentro da sua infraestrutura e fazer sempre um planeamento porque o investimento pode ser curto a dois ou três anos para ter um caminho. Também é importante aumentar a consciencialização dos colaboradores e, depois, toda a parte dos acessos privilegiados porque grande parte dos ataques chega a partir daí"



Bruno Castro, VisionWare: "Por vezes não é possível corrigir vulnerabilidades; temos de arranjar mecanismos alternativos para minimizar o risco dessa falha, até com a prata da casa. O que se aplica são modelos de segurança para minimizar esse impacto. O *budget* é sempre um tema em cima da mesa – antes era muito pior, e agora é mais permeável a esses investimentos. Não faz sentido pensar em nenhum investimento em cibersegurança sem saber o que é que cada empresa tem. É importante cada vez mais sistemas de deteção e reação à medida da organização; um SOC pode não proteger, mas ganha tempo. Por fim, é preciso preparar para o pior"

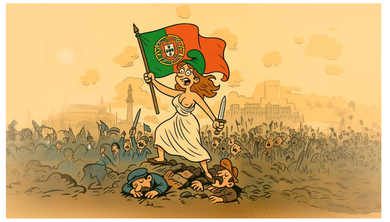
Elizabeth Alves, Exclusive Networks: "Aquilo que vemos muitas vezes são as empresas a comprar soluções *all-in-one* e depois a não saberem utilizar. Isto não compra segurança; compra a ilusão de segurança. Há um dado importante que devia ser visto pelas organizações como um investimento crítico que é o fator humano. A maioria dos incidentes acontece através da pessoa. É preciso apostar na formação e há soluções de *awareness* muito boas. Podemos ter as melhores soluções e consultores, mas, ao final do dia, é o colaborador que está a trabalhar e a ser suscetível a qualquer risco"

ELIZABETH ALVES, SALES DIRECTOR, EXCLUSIVE NETWORKS

"HÁ UM DADO IMPORTANTE QUE DEVIA SER VISTO PELAS ORGANIZAÇÕES COMO UM INVESTIMENTO CRÍTICO QUE É O FATOR HUMANO. A MAIORIA DOS INCIDENTES ACONTECE ATRAVÉS DA PESSOA"

COMO É QUE AS ORGANIZAÇÕES LIDAM COM A ESCASSEZ DE TALENTO EM CIBERSEGURANÇA? QUE COMPETÊNCIAS VEEM EM FALTA NAS ORGANIZAÇÕES MAIS FREQUENTEMENTE?

Miguel Azevedo, Noesis: "De há dois, três anos para cá que temos um desafio adicional que é o facto de Portugal ser um mercado interessante para contratar talento com valores que as empresas portuguesas não conseguem acompanhar. Há projetos que motivam os novos talentos e mantêm as pessoas nas organizações. Há sempre o modelo de serviço – *managed services* – que consegue responder às necessidades de monitorização e operação das organizações"

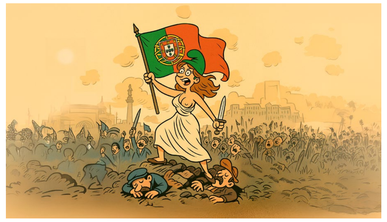


Miguel Barreiros, Securnet: "No problema da escassez de talento começo pelo fim: há um papel das ferramentas automatizadas que podem ajudar as organizações, assim como outras ferramentas avançadas, em algumas matérias. Não resolve por completo, mas ajuda as organizações. Têm existido inúmeras iniciativas de várias entidades para formar mais pessoas e é preciso reconhecer esse esforço; no entanto, há o problema dos outros mercados que competem e pagam melhor do que o nosso. Vão existir coisas que têm de ser colocados fora da organização para entregar algumas das tarefas a alguém especializado"

COM A ENTRADA EM VIGOR DE REGULAMENTAÇÕES COMO A NIS2, QUE MUDANÇAS PRÁTICAS RECOMENDAM ÀS ORGANIZAÇÕES?

David Grave, Claranet Portugal: "Mais do que recomendações, gostava que se mudasse o paradigma da cibersegurança em Portugal. Muitas organizações estão a comprar *checkboxes* para os auditores verem. Gostava que isso mudasse com a NIS2: ter uma cibersegurança que está *compliant* com as normativas, mas também uma cibersegurança efetiva. Temos de falar de risco, do risco do negócio. Falamos muito da tecnologia porque é aquilo que se conhece, mas temos de ajudar os clientes a dar o salto e a falar do risco. É preciso quantificar o ROI, por exemplo. É preciso mudar a narrativa, e isso é responsabilidade do cliente, do regulador, do fabricante e do integrador"

Miguel Barreiros, Securnet: "É preciso formar as competências das pessoas. É preciso uma melhor competência de comunicação dos profissionais de cibersegurança. É adaptar o registo mais técnico ao registo do negócio da organização. Quanto melhor se falar do aspeto do negócio, melhor para todos. A NIS2 não é uma *checklist* para cumprir e nada se resolve dessa forma; é um salto de responsabilização que nos vai obrigar a ter mais maturidade e é fundamental que as empresas mexam nos seus organigramas internos"



RICARDO RODRIGUES, CEO, BALWURK

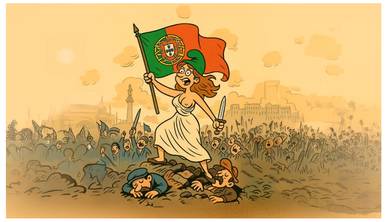
"CONSIDERAMOS QUE HÁ UMA NARRATIVA EXAGERADA DE QUE A IA GENERATIVA VAI SUBSTITUIR AS EQUIPAS DE SEGURANÇA E DE RESPOSTA A INCIDENTES. ACHAMOS QUE ISSO ESTÁ MUITO LONGE DE ACONTECER, MAS ESTÁ AÍ E É PRECISO ADAPTAR"

Ricardo Rodrigues, Balwurk: "As organizações podem preparar-se para a NIS2, mesmo sem existir uma transposição. É uma boa prática. Todos os requisitos que estão especificados na diretiva podem ser seguidos pelas organizações. Para corresponder com a NIS2, a continuidade de negócio é fundamental para cumprir com os requisitos. É preciso identificar todos os ativos organizacionais, mas também precisam de uma gestão contínua. A gestão dos ativos de uma organização tem de ser alimentada para gerir todos os processos. Para existir uma análise do risco também é necessária uma gestão desse mesmo risco"

A IA GENERATIVA É UMA VERDADEIRA REVOLUÇÃO NA CIBERSEGURANÇA OU MAIS *HYPE* DO QUE SUBSTÂNCIA? ONDE VEEM IMPACTO REAL?

Elizabeth Alves, Exclusive Networks: "A inteligência artificial generativa é uma revolução, mas, como todas revoluções, traz luz e sombra. Pelo aspeto positivo, é possível detetar padrões que seriam invisíveis ao olho humano, uma automatização de uma série de processos e um acelerar da resposta a ameaças. Mas também temos uma sombra, porque os cibercriminosos também estão a utilizar IA para criar ataques cada vez mais sofisticados e difíceis de detetar. A inteligência artificial não substitui o ser humano, a supervisão ou a estratégia da organização"

Bruno Castro, VisionWare: "A cibersegurança também era um *hype* aqui há uns anos; esse tempo já passou e o tema da moda é a inteligência artificial. O que temos vindo a ver no mercado nacional é uma adoção rápida de ondas de aplicações de IA. Já utilizamos inteligência artificial para análise forense ou de malware, por exemplo, já há vários anos. Sentimos que vem aí uma nova guerra para quem trabalha na gestão de risco que é a adoção rápida de ferramentas de inteligência artificial que possa automatizar o negócio, o que traz um novo risco para as organizações"



Ricardo Rodrigues, Balwurk: "Os *Large Language Models* são uma novidade transformadora, também para a cibersegurança. Mas há uma diferença entre o potencial em si e a aplicação prática, de como pode passar do *hype* para algo prático, o que é que pode acrescentar à cibersegurança. Consideramos que há uma narrativa exagerada de que a IA generativa vai substituir as equipas de segurança e de resposta a incidentes. Achamos que isso está muito longe de acontecer, mas está aí e é preciso adaptar. É preciso ajudar as organizações a perceber quais os riscos que acarretam quando trazem para os seus sistemas soluções que direta ou indiretamente estão a utilizar inteligência artificial"

David Grave, Claranet Portugal: "O futuro pode ser maravilhoso, ou não. Hoje quase não há produtos que não tenham – ou não digam que têm – IA de alguma maneira integrada. Há, claramente, um *hype*; não há nenhuma tecnologia nova que não tenha algum *hype* associado. É preciso perceber que dados estão a recolher, para onde estão a enviar, mas é inevitável: vamos utilizar inteligência artificial e tem de ser utilizada porque pode ajudar a encontrar determinados padrões. No entanto, se os meus padrões forem fracos, vamos ter uma inteligência artificial fraca"

Miguel Barreiros, Securnet: "A primeira revolução é ao nível dos atacantes. Nas organizações, proibir não funciona; fechar não é solução e incentiva a que se faça ao lado e podemos aprender com as lições aprendidas com o *shadow IT*. É preciso perceber o risco de envenenamento de dados nestes modelos, por exemplo. As aplicações *legacy* são um problema para algumas organizações e a inteligência artificial está a ajudar a refazer essas mesmas aplicações. Esse é um bom exemplo da importância da IA"

MIGUEL BARREIROS, SALES & MARKETING DIRECTOR, SECURNET

"NAS ORGANIZAÇÕES, PROIBIR NÃO FUNCIONA; FECHAR NÃO É SOLUÇÃO E INCENTIVA A QUE SE FAÇA AO LADO E PODEMOS APRENDER COM AS LIÇÕES APRENDIDAS COM O SHADOW IT"

"TER O CUIDADO DE NÃO FICARMOS ARROGANTES. FAZEMOS UM ROADMAP, ESTAMOS NO BOARD, TEMOS ACESSO E O COMPROMISSO DA ORGANIZAÇÃO, MAS TEMOS DE ASSUMIR QUE VAMOS FALHAR E QUE ISTO TUDO VAI CORRER MAL"

SE FOSSEM CISO DE UMA ORGANIZAÇÃO PORTUGUESA HOJE, QUAL SERIA A PRIMEIRA MEDIDA QUE IMPLEMENTARIAM E PORQUÊ?

Ricardo Rodrigues, Balwurk: "A primeira medida que iria implementar era a que fosse capaz de dar a conhecer a minha organização. A primeira medida não pode deixar de ser recorrer à execução de um diagnóstico – que muitas vezes chamamos de auditorias internas – para dar a conhecer o nível de maturidade da segurança de informação e segurança física que me vai permitir identificar necessidades específicas para tomar decisões que vão ao encontro do risco da organização"

Miguel Azevedo, Noesis: "Primeiro é preciso ter visibilidade do risco. Com base nisso, é preciso identificar, fazer a gestão desses ativos, perceber os problemas e as mais-valias e aplicar o que for necessário para mitigar esses mesmos riscos"

David Grave, Claranet Portugal: "Ter o cuidado de não ficarmos arrogantes. Fazemos um *roadmap*, estamos no *board*, temos acesso e o compromisso da organização, mas temos de assumir que vamos falhar e que isto tudo vai correr mal. Quem está no terreno sabe que isto nos torna muito humildes porque não há *silver bullets* para ninguém"

balwurk cyber security

por Ricardo Rodrigues,
CEO, Balwurk

ESTADO DA NAÇÃO – "ENTRE O ALARME E A AÇÃO"

NUM MUNDO ONDE A TRANSFORMAÇÃO DIGITAL ACELERA A UM RITMO SEM PRECEDENTES, A CIBERSEGURANÇA TORNOU-SE NÃO APENAS UMA QUESTÃO TÉCNICA, MAS UMA CONDIÇÃO ESSENCIAL PARA A SUSTENTABILIDADE DOS NEGÓCIOS.

A crescente sofisticação das ameaças digitais obriga as organizações a repensar as suas estratégias de proteção — e, em Portugal, enfrentamos um défice estrutural na proteção digital das nossas organizações, com especial destaque para as PME e para as grandes empresas que, apesar dos investimentos crescentes, continuam vulneráveis.

Os ciberataques são hoje uma inevitabilidade. A questão deixou de ser "se" e passou a ser "quando". Paralelamente, continuamos a lidar com uma perigosa assimetria entre a perceção do risco e a real capacidade de resposta.

As organizações portuguesas, em particular as PME, enfrentam múltiplos obstáculos: escassez de recursos especializados, dificuldade em acompanhar a crescente complexidade tecnológica e ausência de estratégias de segurança bem definidas.

RICARDO RODRIGUES, CEO, BALWURK

O MERCADO DE CIBERSEGURANÇA PERMANECE EXCESSIVAMENTE CENTRADO EM FERRAMENTAS — MUITAS VEZES DISPENDIOSAS E DESAJUSTADAS À REALIDADE LOCAL — EM DETRIMENTO DE ABORDAGENS ADAPTATIVAS, ORIENTADAS PARA O RISCO E PARA A MATURIDADE DE CADA ORGANIZAÇÃO.

Por sua vez, também as grandes empresas não estão imunes. Apesar de dispor de equipas internas e orçamentos mais robustos, continuam a falhar na integração eficaz da segurança ao longo do ciclo de vida do software, na gestão de terceiros e na resposta a incidentes complexos.

A realidade evidencia um "gap" cada vez mais claro entre as soluções disponíveis no mercado e as necessidades concretas das empresas portuguesas.

O mercado de cibersegurança permanece excessivamente centrado em ferramentas — muitas vezes dispendiosas e desajustadas à realidade local — em detrimento de abordagens adaptativas, orientadas para o risco e para a maturidade de cada organização.

É neste contexto que, na **Balwurk**, nos posicionamos como um parceiro estratégico. Não vendemos nem prometemos soluções milagrosas. Oferecemos conhecimento profundo, adaptado ao contexto nacional, com foco na segurança aplicacional, resiliência operacional e maturidade organizacional.

Para as PME, ajudamos a desenhar estratégias de segurança pragmáticas, com um investimento controlado, mas eficaz. Fazemo-lo através de avaliações de risco ajustadas ao negócio, revisão de práticas de desenvolvimento seguro e capacitação de equipas técnicas.

Para grandes empresas, o nosso valor acrescentado reside na Governança da Segurança, no Gap Analysis e em auditorias a frameworks e normas internacionais (como, por exemplo, NIS2, DORA, NIST, ISO 27000, OWASP SAMM, entre outras), bem como na validação contínua da eficácia das medidas implementadas.

Acreditamos que a conformidade regulatória deve ser uma consequência natural de uma boa gestão de risco, e não um exercício meramente burocrático.

A cibersegurança deve ser transversal, contínua e ajustada à realidade. E, acima de tudo, deve deixar de ser vista como um problema do departamento de IT, para passar a ser uma prioridade da Gestão de Topo.

O Estado da Nação exige ação — com estratégia, com foco e com parceiros que compreendam a realidade das empresas.

Na **Balwurk**, estamos prontos para esse desafio.

claranet®

por David Grave,
Security Director da Claranet Portugal

O ESTADO DA NAÇÃO 2025: ENTRE A ILUSÃO DA SEGURANÇA E A REALIDADE DA AMEAÇA

PREOCUPAÇÃO E URGÊNCIA. SÃO ESTAS AS DUAS PALAVRAS QUE MELHOR DEFINEM O VERDADEIRO "ESTADO DA NAÇÃO" EM CIBERSEGURANÇA. NUM CENÁRIO EM QUE AS AMEAÇAS SE SOFISTICAM A UM RITMO SEM PRECEDENTES, PERSISTE EM PORTUGAL UMA PERIGOSA DISSONÂNCIA ENTRE O DISCURSO E A PRÁTICA.

Levantam-se, portanto, questões que, embora desconfortáveis, são necessárias: Estamos realmente preparados para o que aí vem? Ou continuamos confortados por uma falsa sensação de segurança, alimentada por relatórios, apresentações e normas que, na prática, pouco concretizam?

ENTRE O DISCURSO E A REALIDADE: UM DESFASAMENTO PERIGOSO

A imagem que nos é muitas vezes vendida é a de um país que está a "fazer progressos". Mas basta uma análise honesta para perceber que, fora dos setores mais regulados - como a banca ou as telecomunicações -, a maturidade da resposta nacional continua a ser, no melhor dos casos, mediana.

São demasiadas as organizações onde o investimento em *cibersegurança* continua a ser o mínimo necessário para "cumprir requisitos", em vez de uma aposta estratégica. Várias vezes, a segurança é apenas um custo a minimizar - até ao dia em que o prejuízo real surge com a força de um *ransomware* bem-sucedido.

Regulamentos como *NIS2* ou DORA são marcos importantes, mas há um risco real de os vermos como o destino, quando deviam ser o ponto de partida. Cumprir a letra da lei não é sinónimo de estar protegido. **A verdadeira segurança começa onde a conformidade acaba**.


DAVID GRAVE, SECURITY DIRECTOR, CLARANET PORTUGAL

O risco de transformar a regulamentação num exercício de "checkbox" é real - e perigoso. É urgente termos uma governação que encare a *cibersegurança* como parte da continuidade do negócio, não como uma obrigação administrativa.

DA PREPARAÇÃO À PRÁTICA: SABEMOS O QUE FAZER, MAS NÃO FAZEMOS

Hoje, falar de planos de resposta a incidentes é uma prática comum. Mas ter efetivamente um plano testado, com equipas treinadas, é outra coisa. Muitos dirão que têm tudo preparado, mas a realidade é que, muitas vezes, se referem a um PowerPoint esquecido numa pasta, com equipas que nunca fizeram um exercício realista.

Em *cibersegurança*, um "talvez" ou um "em teoria, sim" não chega. Num ataque real, **a hesitação custa tempo, e tempo, neste contexto, custa dados, reputação e dinheiro**.

O FATOR HUMANO NA BASE DA MUDANÇA

Para que a mudança se concretize, é essencial olhar para quem executa a segurança todos os dias - não podemos continuar a ignorar o fator humano.

Portugal sofre de uma escassez crónica de talento em *cibersegurança*. As equipas internas são curtas, sobrecarregadas e muitas vezes ignoradas no processo de decisão, e o investimento na formação e retenção de talento nacional continua a ser insuficiente.

Falar de "resiliência organizacional" sem investir nas pessoas é um paradoxo. E quando falamos em cultura de segurança, precisamos de ir além do e-learning anual. **É preciso criar uma cultura viva de *cibersegurança*, transversal a toda a organização, do estagiário ao CEO**.

Continuamos a dizer que o "elo mais fraco" é o utilizador e a tratá-lo como tal. Vemos campanhas de sensibilização genéricas - sem contexto, sem acompanhamento e sem medição de impacto - e a verdade é que este tipo de estratégia não muda comportamentos.

Se queremos reduzir riscos, temos de envolver os colaboradores no processo de segurança. Precisamos de os capacitar, não apenas de os responsabilizar. E, mais do que tudo, precisamos de começar a medir o sucesso destas iniciativas.

E AGORA? UMA CHAMADA À AÇÃO

Neste cenário complexo, uma coisa é certa: o futuro da *cibersegurança* em Portugal depende, em grande parte, da nossa capacidade de sermos autocríticos. Para tal, precisamos de:

- Abandonar a mentalidade reativa e investir numa abordagem preditiva;
- Encarar a segurança como um fator de competitividade e não como um entrave;
- Reforçar a formação técnica e estratégica das equipas;
- Colocar a *cibersegurança* no centro da governação empresarial;
- Assumir que falhar é possível - e preparar-nos para quando acontecer.

Temos talento, capacidade e acesso à tecnologia. O que nos falta é **prioridade**, **coragem** e **ambição**. Se não aproveitarmos este momento para fazer diferente, não podemos fingir surpresa quando os danos forem reais.

Não há tempo para complacência. Há tempo para decisão. A *cibersegurança* em Portugal está num ponto de viragem: ou damos o salto - estratégico, cultural e operacional - ou vamos continuar a reagir às crises em vez de as evitar.

Assim, a pergunta mais importante a fazer neste momento é: **E nas nossas organizações, estamos focados em manter a ilusão da *segurança*, ou na construção efetiva da resiliência?** ◀

EXCLUSIVE NETWORKS

por Elizabeth Alves, Sales Manager, Exclusive Networks Portugal

MSSP, ZERO TRUST E MICROSEGMENTAÇÃO:

O NOVO TRIPÉ DA CIBERSEGURANÇA EM PORTUGAL

A CIBERSEGURANÇA EM PORTUGAL VIVE HOJE UMA TENSÃO CONSTANTE ENTRE COMPLEXIDADE E URGÊNCIA.

As infraestruturas híbridas, os ambientes cloud, o trabalho remoto e as exigências de compliance (como a NIS2 ou DORA) vieram expor lacunas que não se resolvem com firewalls e antivírus.

Pior: muitas empresas não têm equipas de segurança internas capazes de responder com eficácia a estas exigências.

Perante este cenário, a procura por serviços de cibersegurança geridos (MSSP) tem vindo a crescer de forma sustentada. Estes serviços permitem às organizações aceder a tecnologias de topo, gestão contínua de ameaças e apoio especializado, sem necessidade de investimento inicial elevado.

Através dos MSSP, PME e grandes organizações em Portugal conseguem garantir níveis de proteção que, até há pouco tempo, pareciam inalcançáveis.

E porquê? Porque montar internamente uma estrutura de segurança eficaz implica investimentos pesados em tecnologia, contratação de perfis técnicos escassos, operação 24/7, capacidade de atualização constante e resposta a incidentes em tempo real, algo fora do alcance da maioria das empresas nacionais.

É por isso que muitas organizações começam a colocar a questão essencial: “Será que ainda faz sentido manter tudo in-house? Ou faz mais sentido confiar a operação de segurança a quem tem escala, tecnologia e experiência?”

ELIZABETH ALVES, SALES MANAGER, EXCLUSIVE NETWORKS PORTUGAL

A sua empresa teria capacidade para detetar, isolar e conter um ataque lateral dentro da rede - a meio da noite, sem equipa disponível?

DA TECNOLOGIA AO ECOSSISTEMA: PROTEGER DEIXOU DE SER UMA TAREFA SOLITÁRIA

Nos primeiros anos da cibersegurança, bastava instalar ferramentas: firewall, antivírus, antispam. A proteção era feita por tecnologia. Hoje, isso já não chega. A complexidade dos ambientes, a velocidade das ameaças e a escassez de talento obrigam as empresas a pensar não em produtos, mas em ecossistemas: conjuntos de soluções que falam entre si, operadas por parceiros de confiança, com suporte contínuo e visão estratégica.

E é precisamente aí que o modelo MSSP e a lógica de ecossistema se cruzam. Para muitas empresas, o desafio já não está em escolher o produto certo, está em garantir que a arquitetura, os serviços e os recursos certos estão alinhados e integrados.

O desafio? Mapear tudo, identificar, perceber, gerir, manter, monitorizar, desenhar a melhor solução. Muitos dos problemas que surgem devem-se a soluções mal dimensionadas, à falta de recursos e de know-how para as gerir. Não basta instalar uma solução e dar o processo como concluído.

Neste novo contexto torna-se essencial contar com um parceiro que compreenda a realidade do terreno e ajude a traduzi-la em soluções concretas. “Tão importante como a tecnologia é o trabalho de proximidade: a consultoria, a formação, a gestão, a manutenção e a monitorização das ferramentas. Sempre acompanhámos os nossos clientes e parceiros em todo o processo. Por isso, sabemos que o nosso apoio é decisivo para o sucesso de cada implementação”, sublinha Elizabeth Alves, Sales Manager, Exclusive Networks Portugal.

“A Exclusive Network mantém uma presença sólida junto do canal e dos fabricantes, e tem vindo a trabalhar lado a lado com os seus parceiros para desenhar estratégias de segurança ajustadas ao perfil e maturidade de cada organização. Esse trabalho inclui desde o aconselhamento técnico e comercial, até ao apoio direto na construção e operação de ofertas geridas, sempre com foco na integração eficaz de tecnologias de segurança, cloud e infraestrutura.”

ZERO TRUST: CONFIAR APENAS NO QUE É VERIFICÁVEL

No centro da transformação da segurança digital está o modelo Zero Trust, que parte de um princípio claro: não confiar por defeito em nenhum utilizador, ou aplicação — mesmo dentro da rede corporativa.

A lógica é simples, mas a sua implementação exige mais do que uma mudança tecnológica — implica uma nova forma de pensar a confiança, o acesso e o risco.

Durante anos, a maioria das infraestruturas digitais baseou-se na ideia de perímetro: tudo o que estava “dentro” era considerado seguro. Mas o crescimento da cloud, do trabalho remoto e das aplicações distribuídas tornou esse modelo obsoleto.

Hoje, os ataques acontecem dentro da rede tanto quanto fora dela e, muitas vezes, são silenciosos, persistentes e quase invisíveis.

É aqui que o Zero Trust se torna relevante: ao aplicar verificação contínua, controlo granular de acessos e monitorização baseada em contexto, reduz drasticamente a superfície de ataque.

Mas para que este modelo funcione na prática, é necessário mais do que política: é preciso arquitetura.

É aí que entra a microsegmentação como componente-chave. Ao permitir isolar zonas críticas da infraestrutura, evita movimentos laterais de atacantes, limita o acesso indevido e reduz o impacto de qualquer incidente a uma fração mínima. Em vez de proteger "tudo de uma vez", protege-se o que é preciso, quando é preciso, com base em regras claras.

MICROSEGMENTAÇÃO QUE FUNCIONA, SEM COMPLICAÇÕES

Implementar microsegmentação sempre foi visto como um processo moroso e complexo. Durante anos, exigiu alterações à infraestrutura, instalação de agentes, mapeamento manual de acessos e um investimento técnico considerável, algo muitas vezes fora do alcance de equipas reduzidas.

É neste ponto que surgem novas soluções pensadas para a realidade do terreno. Um exemplo claro é o da tecnologia de microsegmentação automatizada recentemente integrada no portefólio da Exclusive Networks, com foco na eliminação de complexidade técnica e redução do tempo de implementação.

Uma das soluções mais relevantes neste contexto é a da Zero Networks, que permite criar políticas de acesso com base no comportamento real dos utilizadores e aplicações, sem agentes, e com integração direta com ambientes Microsoft e Active Directory. O processo é quase invisível para o utilizador final, mas altamente eficaz na contenção de riscos e acessos não autorizados.

"Esta solução permite ativar segurança lateral e segmentação de aplicações críticas em apenas dias, sem fricção operacional. É o tipo de abordagem que o mercado português valoriza - simples, eficaz e com retorno visível", acrescenta Elizabeth Alves.

Para muitas empresas portuguesas, especialmente aquelas que não têm uma equipa de cibersegurança dedicada, esta abordagem representa um salto qualitativo imediato. Permite aplicar os princípios do Zero Trust de forma prática e escalável, sem reformular toda a arquitetura da rede. E, sobretudo, liberta as equipas para se concentrarem na operação, e não na complexidade da proteção.

5 SINAIS DE QUE ESTÁ NA HORA DE EVOLUIR

- A equipa de IT não tem recursos para gerir alertas 24/7
- A proteção atual depende de perímetros fixos ou confiança implícita
- O controlo de acessos entre departamentos é inexistente
- Os requisitos de compliance aumentaram (NIS2, DORA)
- A visibilidade lateral da rede é praticamente nula

Se respondeu "sim" a 2 ou mais pontos, é provável que a sua empresa **precise de repensar a estratégia de cibersegurança**.

SEGURANÇA EFICAZ É SEGURANÇA INTEGRADA

A cibersegurança eficaz já não se constrói com camadas soltas de tecnologia. Constrói-se com visão estratégica, simplicidade operacional e integração real entre soluções e serviços.

"É este o princípio que orienta o trabalho da Exclusive Networks com os seus parceiros e fabricantes. O objetivo é sempre ajudar o mercado a evoluir de modelos reativos para arquiteturas de proteção coordenada, adaptadas às necessidades reais das organizações."

Ao combinar soluções líderes com conhecimento técnico local, a EXN ajuda empresas em Portugal a implementar estratégias Zero Trust, microsegmentação e serviços MSSP com retorno visível, sem complicações desnecessárias. ◀

noesis
an Altia Company

por José Gomes, IT Operations, Cloud & Security Associate Director

CIBERSEGURANÇA EM PORTUGAL: ENTRE O PROGRESSO E A URGÊNCIA DE MUDANÇA

A TEMÁTICA DA CIBERSEGURANÇA NÃO DEVE SER LEVADA COMO UM TEMA TÉCNICO, MAS ANTES UMA QUESTÃO ESTRATÉGICA, ESSENCIAL À RESILIÊNCIA DAS ORGANIZAÇÕES, ENVOLVENDO, INCLUSIVE, A SOBERANIA DIGITAL DOS PAÍSES.

Em Portugal, o panorama da cibersegurança tem mostrado avanços significativos, especialmente nas grandes empresas e no setor público. No entanto, **apesar de muitas organizações estarem a reforçar as suas capacidades digitais de cibersegurança com ferramentas modernas de proteção dos seus ativos, incluindo sistemas "inteligentes" de deteção de ameaças, autenticação multifator e monitorização em tempo real, ainda estamos a meio da jornada**.

Os números do relatório "*Cybersecurity Market Report 2024*", da IDC Portugal, falam por si: o investimento em cibersegurança cresceu cerca de 35% em 2024 e **estima-se que aumente mais 40% em 2025**, existindo sinais claros de que proteger sistemas e dados passou a ser uma prioridade estratégica. Além disso, as novas regras da União Europeia, como a diretiva NIS 2 e o regulamento DORA, assumem um papel fundamental nesta tomada de consciência ao exigirem às empresas processos de segurança mais sólidos e uma abordagem mais rigorosa à gestão de riscos.

Não obstante, há uma fatia muito significativa do mercado que ainda nem começou a pensar em cibersegurança. Muitas pequenas e médias empresas (PME) – consideradas a espinha dorsal da economia portu-

JOSÉ GOMES, IT OPERATIONS, CLOUD & SECURITY ASSOCIATE DIRECTOR

OS NÚMEROS DO RELATÓRIO "*CYBERSECURITY MARKET REPORT 2024*", DA IDC PORTUGAL, FALAM POR SI: O INVESTIMENTO EM CIBERSEGURANÇA CRESCEU CERCA DE 35% EM 2024 E ESTIMA-SE QUE AUMENTE MAIS 40% EM 2025, EXISTINDO SINAIS CLAROS DE QUE PROTEGER SISTEMAS E DADOS PASSOU A SER UMA PRIORIDADE ESTRATÉGICA

guesa – continuam a confiar cegamente nos provedores de soluções, suportando os seus negócios em **sistemas obsoletos, redes mal segmentadas e software desatualizado**. A verdade é que a maioria destas PME não possui (sequer) equipas dedicadas à segurança e carece de ferramentas básicas como firewalls avançadas, ferramentas de gestão de acessos privilegiados, soluções de backup fiáveis ou antivírus com capacidades de deteção inteligente.

Ainda mais alarmante é a falta de consciência e de preparação generalizadas que persistem em muitas organizações. De acordo com o estudo "Cibersegurança em Portugal 2023", do Centro Nacional de Cibersegurança (CNCS), **cerca de 12% das entidades desconhecem por completo as obrigações legais da diretiva NIS 2 e 40% das lideranças nunca receberam qualquer formação em cibersegurança**. Este défice de literacia cibernética torna estas organizações especialmente vulneráveis a ataques que exploram fragilidades básicas, como palavras-passe fracas, mensagens de *phishing* ou falhas simples de atualização de software.

Estamos perante uma falha estrutural que **não se resolve apenas com tecnologia**. A cibersegurança começa nas pessoas e, por isso, a literacia digital e a capacitação técnica devem estar no centro das prioridades de política pública. **É urgente reforçar a articulação entre os setores público e privado e o meio académico**, criando uma aliança eficaz que partilhe conhecimento, alinhe esforços e acelere a formação de talento especializado, à altura dos riscos que já enfrentamos e daqueles que, inevitavelmente, se avizinham.

A crescente digitalização da sociedade portuguesa torna urgente reforçar a cibersegurança no país, não só para proteger dados pessoais e empresariais, mas também para **garantir a segurança das infraestruturas críticas** que sustentam o nosso quotidiano. Sem ações concretas e coordenadas, arriscamo-nos a comprometer a confiança digital.

O risco é permanente, mas também coletivo. Ignorar estas vulnerabilidades deixa não só as empresas expostas, mas fragiliza o ecossistema digital nacional como um todo. ◀

SECURNET
ALWAYS ONLINE | ALWAYS SECURE

por Miguel Barreiros,
Sales & Marketing Director da SECURNET

ALWAYS SMART

A IMPORTÂNCIA DO CONHECIMENTO, DO TREINO E DO RACIOCÍNIO HUMANO NA ERA DA INTELIGÊNCIA ARTIFICIAL.

Com a **Inteligência Artificial**, sem qualquer tipo de dúvida, **uma das forças mais transformadoras dos nossos tempos**, estamos a assistir a uma revolução, tão silenciosa quanto profunda, nas vantagens competitivas concretas das organizações, mas também nos nossos comportamentos.

Muitos têm sido os estudos, artigos e debates sobre a importância e o papel da IA generativa na cibersegurança. Em alguns deles, a IA generativa é considerada a mais recente maravilha que substituirá humanos, com "agentes do bem" capazes de lutar contra o cibercrime tal qual o fariam os heróis da Marvel ou da DC Comics. Mas será exatamente assim?

É também assegurada a tentação das organizações de apostarem em soluções baseadas nos hypes do mercado, muito influenciadas pelo poder da comunicação dos principais atores do setor, sem que tenham internamente consolidados fundamentos e cultura de cibersegurança. Organizações com baixa maturidade tecnológica tendem a procurar atalhos tecnológicos ao invés de investirem em políticas, processos e pessoas.

Olhemos primeiramente a alguns dos riscos emergentes e ao real impacto da IA generativa. O cibercrime organizado está, como sempre, na linha da frente e entre os usos mais preocupantes destacam-se:

- **Phishing de altíssima qualidade**, com uma enorme taxa de sucesso, com e-mails e mensagens praticamente indistinguíveis aos utilizadores.

• **Deepfakes e voice cloning** usados em fraudes BEC (Business Email Compromise) ou ataques dirigidos ao C-Level, de que são exemplo **Fraude do CEO**, a **manipulação de faturas** ou o **roubo de credenciais**.

• Automatização da **engenharia social**, com chatbots maliciosos ou campanhas segmentadas em larga escala por agentes de IA.

• Os **ataques de negação de serviço** (DDoS), orquestrados e reinventados por atores autónimos e incansáveis, com recursos quase ilimitados ao seu dispor.

Mas em igual medida em que os riscos estão aí, também há muito boas notícias e os recursos defensivos têm escalado para potentes meios de cibersegurança, com irrefutáveis benefícios como:

• **Deteção e resposta automatizada**, com as ferramentas de EDR, NDR, MDR e XDR e similares, bem como os SIEM a incorporarem modelos generativos que tratam alertas complexos, priorizam riscos e sugerem até ações corretivas automáticas.

• **Análise de malware** e **threat intelligence**, com a IA generativa a apoiar os analistas na reversão de código malicioso, identificação de variantes e previsão de vetores de ataque com base em padrões observados, dando eficiência e uma incrível redução nos tempos de resposta das análises forenses.

• **Formação**, **sensibilização** e **treino personalizados**, com plataformas de simulação que através da IA generativa começam a criar cenários de phishing ou ataques internos adaptados ao contexto de cada organização, ou mesmo concebendo planos individuais adaptados às maiores fragilidades identificadas em cada utilizador, naquela que é ainda a maior vulnerabilidade da maioria das empresas.

Em conclusão, a IA generativa por si só, não resolve problemas estruturais como a falta de backups testados, de políticas de identidade e acesso ou a gestão de vulnerabilidades. Sem uma base sólida será apenas mais uma camada sobre problemas mal resolvidos. Contudo, a capacidade de criar novos conteúdos baseados no tratamento e correlação de dados em quantidades estratosféricas, num espaço de tempo antes inimaginável, vem acrescentar novos "superpoderes" aos comuns dos mortais que **precisam de saber**, de **ser capacitados** e **muito bem treinados** de como melhor os utilizar.

Não caminhamos para a substituição dos profissionais humanos, mas têm que estar bastante mais atentos e bastante mais bem preparados para enfrentar os riscos potenciados pela IA generativa, têm que ser **capacitados para utilizar ferramentas cada vez mais inteligentes, mais potentes e mais eficazes**, mas também mais generalizadamente ao seu dispor.

A SECURNET tem na sua assinatura desde há muitos anos o mote "**Always Online, Always Secure**". Terá chegado o momento de acrescentar o desígnio de "**ALWAYS SMART**"!

Para mais informações, contacte-nos em:
info@securnet.pt ◀

VisionWare since 2005

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

DESINFORMAÇÃO E RESILIÊNCIA DEMOCRÁTICA

NA ERA EM QUE A INFORMAÇÃO CIRCULA À VELOCIDADE DA LUZ, A VERDADE NEM SEMPRE ACOMPANHA ESSE RITMO.

A desinformação tornou-se uma das ameaças híbridas mais insidiosas à "saúde" das democracias contemporâneas. Não se trata apenas de boatos inofensivos ou teorias marginais: a desinformação é hoje uma ferramenta ao serviço da guerra híbrida, utilizada por atores estatais e não estatais, para dividir, manipular e corroer a confiança nas instituições democráticas.

A desinformação infiltra-se onde a democracia é mais vulnerável: na opinião pública. Num ambiente digital onde as redes sociais amplificam conteúdos emocionais e sensacionalistas, factos e ficções misturam-se num caos digital que dificulta a deliberação racional. Quando milhões de pessoas partilham uma mentira, ela ganha uma força social que desafia até as instituições mais sólidas e é precisamente essa, a intenção dos promotores da desinformação, isto é, minar a coesão social, semear a desconfiança e desmobilizar a cidadania informada. Em eleições, por exemplo, notícias falsas sobre candidatos, manipulações de contexto, proliferação de deepfakes ou campanhas de difamação podem distorcer resultados, desacreditar sistemas eleitorais e até polarizar irremediavelmente o debate público.

Face a este cenário, a questão não é apenas como combater a desinformação, mas sim, como fortalecer a resiliência das democracias. Resiliência, neste contexto, não se limita à capacidade de absorver choques. Implica também a aptidão para aprender com eles, já que, uma sociedade resiliente não é imune à mentira, mas deve antes saber reconhecê-la, enfren-

BRUNO CASTRO, VISIONWARE

A LITERACIA MEDIÁTICA DEVE TORNAR-SE UMA PRIORIDADE TRANSVERSAL, DESDE O ENSINO BÁSICO ATÉ À FORMAÇÃO CONTÍNUA DE ADULTOS. PROMOVER O PENSAMENTO CRÍTICO, CAPACITAR PARA O USO ÉTICO DAS REDES SOCIAIS E DESENVOLVER SENSIBILIDADE PARA OS SINAIS DE MANIPULAÇÃO SÃO FERRAMENTAS ESSENCIAIS PARA IMUNIZAR A SOCIEDADE.

tá-la e superá-la através da educação, do pluralismo mediático e de instituições transparentes.

A resposta europeia a este desafio tem evoluído de forma significativa. A União Europeia (UE) reconheceu cedo que a desinformação não é apenas uma questão de liberdade de expressão, mas antes uma ameaça à soberania democrática. Ao longo do tempo têm sido adotadas medidas concretas para enfrentar esta ameaça, com destaque para a criação do Plano de Ação contra a Desinformação (2018), que visou aumentar a deteção precoce, promover a cooperação entre Estados-Membros e reforçar a responsabilização das plataformas digitais.

Já em 2022, a entrada em vigor do Código de Conduta reforçado sobre a Desinformação, direcionado também a grandes plataformas como a Google, Meta e TikTok, introduziu obrigações mais rigorosas, como a transparência nos algoritmos, o combate à monetização de conteúdos falsos e a verificação por entidades independentes. Por outro lado, a Lei dos Serviços Digitais (DSA), em vigor desde 2024, estabelece deveres legais de moderação de conteúdos e gestão de riscos sistémicos, incluindo a propagação de desinformação em grande escala.

Além disso, a UE tem investido em literacia mediática e criou também equipas especializadas, como o East StratCom Task Force, responsável por monitorizar campanhas de desinformação vindas do exterior, especialmente da Rússia, e produzir relatórios regulares sobre as suas táticas e narrativas.

Contudo, estas medidas só serão eficazes se forem acompanhadas por um esforço coordenado a nível nacional e local. A primeira linha de defesa contra a desinformação continua a ser a cidadania.

A literacia mediática deve tornar-se uma prioridade transversal, desde o ensino básico até à formação contínua de adultos. Promover o pensamento crítico, capacitar para o uso ético das redes sociais e desenvolver sensibilidade para os sinais de manipulação são ferramentas essenciais para imunizar a sociedade.

Importa ainda reconhecer que a desinformação não é apenas um problema técnico, mas antes profundamente político. Alimenta-se de desigualdades, de ressentimentos e de desilusões com o funcionamento da democracia. Por isso, construir resiliência democrática passa também por fortalecê-la com ações concretas que envolvam educação, regulação, transparência e responsabilidade coletiva. No fim de contas, proteger a verdade, é proteger a liberdade. ◀

DECRETO-LEI DE ENTIDADES CRÍTICAS:
DA OBRIGAÇÃO LEGAL À VANTAGEM COMPETITIVA

POR INÊS GARCIA MARTINS

POR ENTRE A VAGA DE REGULAÇÃO QUE A EUROPA TEM ASSISTIDO, O NOVO DECRETO-LEI DE ENTIDADES CRÍTICAS (DECRETO-LEI N.º 22/2025) SURGE COMO PARADOXO PARA AS EMPRESAS PORTUGUESAS. MAIS DO QUE UM DESAFIO DE CONFORMIDADE, IMPÕE OBRIGAÇÕES QUE VÃO ALÉM DA CIBERSEGURANÇA E EXIGEM MUDANÇAS PROFUNDAS NA GESTÃO DO RISCO. A RESPOSTA NÃO É SIMPLES, SOBRETUDO QUANDO OS ESPECIALISTAS ALERTAM PARA UM NÍVEL MÍNIMO DE PREPARAÇÃO. MESMO ASSIM, ESTE NOVO ENQUADRAMENTO PODE TRANSFORMAR-SE DE OBRIGAÇÃO EM VANTAGEM COMPETITIVA PARA QUEM SOUBER ANTECIPAR-SE

Num cenário global de "policrise", marcado por ameaças híbridas, disrupções nas cadeias de abastecimento e a crescente sofisticação dos ciberataques, o panorama regulatório português prepara-se para uma mudança estrutural. A iminente implementação do Decreto-Lei n.º 22/2025, que estabelece o regime de resiliência das entidades críticas, é a resposta nacional a este desafio. Longe de ser apenas mais um diploma a arquivar, esta legislação, que transpõe a Diretiva (UE) 2022/2557 (Diretiva CER), representa uma redefinição fundamental da forma como as organizações vitais para o país devem encarar e gerir o risco. Para os profissionais de cibersegurança e gestão de risco, o desafio é claro: transformar uma complexa teia de obrigações numa alavanca estratégica para a resiliência operacional e o ganho competitivo.

O novo quadro legal, como resume de forma sucinta Daniel Reis, Sócio da DLA Piper, "cria um novo quadro jurídico para identificar, designar e reforçar a resiliência das entidades críticas nacionais e europeias, para garantir a continuidade de serviços essenciais. De forma simplista, vem criar obrigações para as entidades críticas". Esta aparente simplicidade esconde, no entanto, uma profundidade de mudança que vai muito além da cibersegurança, o que, por sua vez, exige uma abordagem integrada que poucas empresas em Portugal já praticam de forma sistemática.


DANIEL REIS, DLA PIPER

UMA VISÃO HOLÍSTICA DO RISCO

A principal novidade prática deste Decreto-Lei é a sua abrangência. Ao contrário de regimes como a NIS2, que se foca especificamente na segurança digital, esta legislação impõe uma gestão de risco que transcende as barreiras do digital e do físico, o que força uma colaboração sem precedentes entre diferentes departamentos.

O NOVO QUADRO LEGAL, "CRIA UM NOVO QUADRO JURÍDICO PARA IDENTIFICAR, DESIGNAR E REFORÇAR A RESILIÊNCIA DAS ENTIDADES CRÍTICAS NACIONAIS E EUROPEIAS, PARA GARANTIR A CONTINUIDADE DE SERVIÇOS ESSENCIAIS. DE FORMA SIMPLISTA, VEM CRIAR OBRIGAÇÕES PARA AS ENTIDADES CRÍTICAS".

Catarina Mascarenhas, Consultora da Abreu Advogados, detalha esta mudança de paradigma, e explica que as empresas vão enfrentar "um conjunto de obrigações que recaem sobre a entidade crítica, como um todo, enquanto organização, recursos humanos e modo de funcionamento, assente numa lógica de gestão de risco". Lógica essa que exige, segundo a especialista, uma "visão holística, integrada e coordenada perante um conjunto de ameaças e riscos que vão desde atos intencionais a catástrofes naturais e a emergências de saúde pública".

Isto significa que o CISO e o responsável pela segurança física, que em muitas organizações operam em silos, terão de se sentar à mesma mesa e desenvolver estratégias conjuntas. O plano de resiliência de um operador de infraestruturas de transportes, por exemplo, terá de contemplar tanto a defesa contra um ataque de ransomware que paralise os seus sistemas de logística, como a resposta a uma greve que afete a operação ou a um

evento climático extremo que danifique as suas infraestruturas.

As obrigações são claras e exigentes: realizar avaliações de risco que abranjam todo o espectro de ameaças, elaborar planos de resiliência que contemplem medidas preventivas, de proteção, resposta e recuperação, e testá-los através de exercícios periódicos. Adicionalmente, a notificação de incidentes com impacto significativo deve ser feita no prazo máximo de 24 horas. Por fim, como nota Catarina Mascarenhas, estas entidades estão também "sujeitas a ações de fiscalização como auditorias e inspeções", o que eleva o nível de escrutínio e responsabilidade a um novo patamar.

O ROTEIRO PARA A DESIGNAÇÃO E O PUZZLE REGULATÓRIO

Uma das questões centrais para as empresas é saber se são abrangidas. O processo, conduzido pelo Conselho Nacional de Planeamento Civil de Emergência (CNPCE) em articulação com as entidades setoriais, tem um prazo definido. "A identificação e designação devem ocorrer até 17 de julho de 2026", clarifica José Maria Alves Pereira, Advogado Principal da Abreu Advogados. Os critérios para ser considerada "crítica" são cumulativos e incluem a prestação de serviços essenciais, a operação em território nacional e, crucialmente, a avaliação de que um incidente provocaria um "efeito perturbador significativo".


CATARINA MASCARENHAS, ABREU ADVOGADOS

"A NIS 2 É ESPECÍFICA PARA A CIBERSEGURANÇA, ENQUANTO O DECRETO-LEI N.º 22/2025 ADOTA UMA ABORDAGEM MAIS ABRANGENTE, INCLUINDO TANTO AMEAÇAS FÍSICAS COMO CIBERNÉTICAS"


MAFALDA DE BRITO FERNANDES, CUATRECASAS

Mafalda de Brito Fernandes, Advogada da Cuatrecasas, detalha que este impacto será avaliado com base em métricas concretas como "o número de utilizadores afetados, interdependências setoriais, impacto socioeconómico, quota de mercado e vulnerabilidades geográficas".

Para os profissionais de cibersegurança, a articulação deste regime com a Diretiva NIS2 é vital – não são regimes conflituantes, mas sim complementares. "A NIS 2 é específica para a cibersegurança, enquanto o Decreto-lei n.º 22/2025 adota uma abordagem mais abrangente, incluindo tanto ameaças físicas como cibernéticas", reforça Catarina Mascarenhas. Na prática, uma entidade crítica terá de cumprir ambos, através da montagem de um complexo *puzzle* regulatório que, em setores como o financeiro, inclui ainda uma terceira peça fundamental. "Importa salientar que no campo das entidades financeiras estas matérias, face ao princípio da especialidade, se encontram reguladas no DORA (Digital Operational Resilience Act)", acrescenta Catarina Mascarenhas.

> PARA EMPRESAS DOS SETORES DA ENERGIA, TELECOMUNICAÇÕES E FINANCEIRO, "A ADAPTAÇÃO DESTAS ENTIDADES NÃO SERÁ NENHUM 'BICHO DE SETE CABEÇAS'", UMA VEZ QUE JÁ POSSUEM POLÍTICAS DE GESTÃO DE RISCO AVANÇADAS. "DE TODO O MODO, NÃO DEIXA DE SER MAIS UM DECRETO-LEI QUE AS ENTIDADES TERÃO DE ANALISAR, DOMINAR E ADAPTAR À SUA REALIDADE, O QUE APENAS REFORÇA A IMPORTÂNCIA REGULATÓRIA DA CIBERSEGURANÇA NO CONTEXTO ATUAL",

O PESO DAS SANÇÕES E A GOVERNANÇA DO RISCO

O incumprimento não será uma opção, uma vez que o legislador dotou o regime de um arsenal sancionatório desenvolvido para garantir a sua aplicação efetiva. José Maria Alves Pereira explica que, perante uma suspeita, o processo pode começar de forma pedagógica: "as entidades críticas poderão ser sujei-

tas a advertências", contendo as normas infringidas e as medidas corretivas a implementar.

Contudo, a persistência na falha pode levar à "aplicação de coimas pelas infrações praticadas, além de sanções pecuniárias compulsórias enquanto se mantiver a infração".

Esta última ferramenta, em particular, pode representar um encargo financeiro contínuo e pesado para as organizações que adiem a conformidade. A fiscalização e aplicação destas sanções caberá ao Secretário-Geral do Sistema de Segurança Interna, solidificando a governança do regime.

DA RESILIÊNCIA À VANTAGEM COMPETITIVA EM SETORES SENSÍVEIS

Encarar este Decreto-Lei apenas como um fardo de conformidade é um erro estratégico, já que as empresas que abraçarem a resiliência como um pilar da sua operação podem colher benefícios significativos.

JOSÉ MARIA ALVES PEREIRA, ABREU ADVOGADOS

Pensemos no setor da energia. Um produtor ou distribuidor que demonstre, através de planos robustos e exercícios testados, a sua capacidade de manter o fornecimento durante uma crise – seja um ciberataque, uma falha de equipamento ou uma seca prolongada – não está apenas a cumprir a lei. Está a oferecer uma garantia de fiabilidade aos seus clientes industriais e a posicionar-se como um parceiro mais seguro nas cadeias de abastecimento europeias.

PERANTE UMA SUSPEITA, O PROCESSO PODE COMEÇAR DE FORMA PEDAGÓGICA: "AS ENTIDADES CRÍTICAS PODERÃO SER SUJEITAS A ADVERTÊNCIAS", CONTENDO AS NORMAS INFRINGIDAS E AS MEDIDAS CORRETIVAS A IMPLEMENTAR. CONTUDO, A PERSISTÊNCIA NA FALHA PODE LEVAR À "APLICAÇÃO DE COIMAS PELAS INFRAÇÕES PRATICADAS, ALÉM DE SANÇÕES PECUNIÁRIAS COMPULSÓRIAS ENQUANTO SE MANTIVER A INFRAÇÃO".

Na saúde, um grande grupo hospitalar cuja resiliência garanta a continuidade dos serviços, mesmo perante uma falha sistémica de IT, reforça a confiança dos utentes e do Estado. Já no setor dos transportes, um porto que consiga manter as suas operações logísticas a funcionar após um incidente grave torna-se um nó mais fiável e atrativo na rede de comércio internacional. Esta capacidade de "assegurar a continuidade de serviços essenciais e a proteção das infraestruturas críticas", como refere Mafalda de Brito Fernandes, torna-se um diferenciador de mercado.

ESTAMOS PREPARADOS?

A questão da preparação nacional é, contudo, a grande incógnita. A opinião dos especialistas sugere uma realidade a duas velocidades. Mafalda de Brito Fernandes oferece uma perspetiva otimista para os setores mais maduros, afirmando que para empresas dos setores da energia, telecomunicações e financeiro, "a adaptação destas entidades não será nenhum 'bicho de sete cabeças'", uma vez que já possuem políticas de gestão de risco avançadas. "De todo o modo, não deixa de ser mais um Decreto-Lei que as entidades terão de analisar, dominar e adaptar à sua realidade, o que apenas reforça a importância regulatória da cibersegurança no contexto atual", adverte a advogada. Para muitas outras entidades, a implementação vai ser um projeto complexo, que vai exigir investimento e uma mudança cultural profunda.

A esta análise, que aponta para uma preparação a duas velocidades, Daniel Reis acrescenta um realismo pragmático que funciona como um alerta. A sua resposta é clara e direta: neste momento, as entidades não estão preparadas. Baseia-se num facto que afeta tanto os mais preparados como os que partem de trás, algo que "não é surpreendente visto estarmos perante obrigações legais novas, e um quadro legal que ainda carece de concretização. Por exemplo, ainda não foi publicada a Estratégia Nacional para a Resiliência das Entidades Críticas, a aprovar aprovadas por resolução do Conselho de Ministros", revela o Sócio da DLA Piper.

O novo regime é, em suma, um ponto de viragem que força as organizações a olharem para o risco de uma forma integrada. Para os profissionais que lideram este esforço, a missão evoluiu: já não se trata apenas de garantir a conformidade para mitigar o risco legal, mas de usar este impulso regulatório para construir organizações genuinamente mais fortes, seguras e competitivas.

por CSO Team

AUTOMAÇÃO NA RESPOSTA A INCIDENTES:

ESTRATÉGIAS PARA EQUIPAS MODERNAS DE CIBERDEFESA

NUM CENÁRIO ONDE AS AMEAÇAS DIGITAIS EVOLUEM À VELOCIDADE DA LUZ, AS EQUIPAS DE RESPOSTA A INCIDENTES ENFRENTAM PRESSÕES CRESCENTES PARA ATUAR COM RAPIDEZ, PRECISÃO E EFICIÊNCIA. A AUTOMAÇÃO TEM-SE REVELADO UMA FERRAMENTA ESTRATÉGICA ESSENCIAL PARA ALCANÇAR ESTES OBJETIVOS. A SUA ADOÇÃO MARCA UMA MUDANÇA DE PARADIGMA NA FORMA COMO AS ORGANIZAÇÕES ENCARAM A CIBERDEFESA OPERACIONAL.

A crescente sofisticação das ciberameaças obriga as equipas de segurança a adotarem abordagens cada vez mais proativas e dinâmicas. A literatura científica tem consistentemente apontado a automação como um dos principais aceleradores de maturidade nos Security Operations Centers (SOCs). Estudos recentes (por exemplo, P. Lemos et al., 2023, IEEE Transactions on Information Forensics and Security) demonstram que a adoção de plataformas de Security Orchestration, Automation and Response (SOAR) pode reduzir em até 80% o tempo médio de resposta (MTTR) em incidentes comuns.

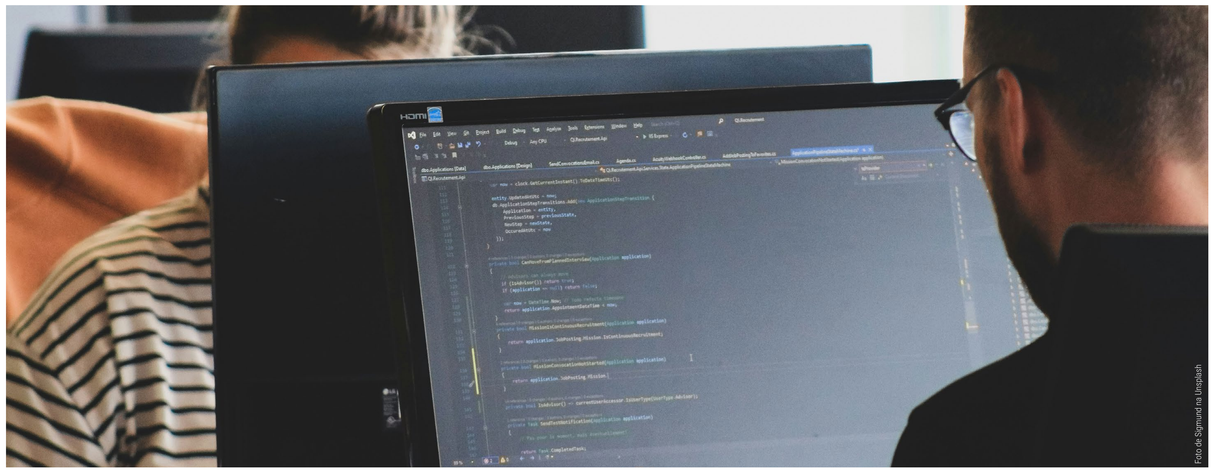


Foto de Sigmund na Unsplash

É FUNDAMENTAL CAPACITAR OS ANALISTAS NÃO APENAS NO USO DAS FERRAMENTAS, MAS TAMBÉM NA INTERPRETAÇÃO CRÍTICA DAS AÇÕES AUTOMATIZADAS

As plataformas SOAR integram ferramentas de deteção, fontes de inteligência de ameaças, scripts automatizados, entre outros recursos, permitindo não apenas a correlação de eventos em larga escala, mas também respostas automatizadas com mínima intervenção humana. Isso liberta os analistas de tarefas repetitivas e sujeitas a erro, como a análise inicial de logs ou o bloqueio de IPs maliciosos.

Contudo, a automação não deve ser encarada como substituição das capacidades humanas, mas sim como um multiplicador de eficácia. A integração de Machine Learning para detetar padrões anómalos e o uso de playbooks baseados em regras de negócio são exemplos de como a automação pode ser ajustada para refletir o contexto organizacional. Mais recentemente, algoritmos de inteligência artificial têm sido incorporados nestes playbooks, permitindo decisões mais adaptativas, contextuais e baseadas em histórico de incidentes reais, respeitando sempre políticas e limites operacionais.

Apesar dos benefícios tangíveis, a adoção de automação exige uma abordagem estratégica e multidisciplinar. A gestão de risco recomenda, por exemplo, a análise de impacto de cada ação automatizada. Um bloqueio automático de um endereço IP pode, se mal contextualizado, interromper serviços críticos.

Uma estratégia eficaz deve começar com a identificação de casos de uso prioritários — como resposta a phishing, análise de malware ou gestão de vulnerabilidades. Para cada um, é crucial desenvolver playbooks baseados em processos já bem definidos e testados manualmente. A validação contínua é outro ponto crítico: os algoritmos de automação devem ser auditáveis e atualizados à medida que as ameaças evoluem.

Além disso, o fator humano continua a ser central. É fundamental capacitar os analistas não apenas no uso das ferramentas, mas também na interpretação crítica das ações automatizadas. As melhores práticas sugerem modelos híbridos de decisão, em que a automação atua até certo ponto e depois transfere o controlo para o analista.

Sem dúvida que deve haver um alinhamento claro entre a automação e os objetivos estratégicos da organização. Isso inclui o cumprimento de requisitos de conformidade (como o RGPD), a proteção da reputação institucional e o fortalecimento da resiliência operacional.

Em jeito de conclusão, a automação, quando bem planeada e implementada de forma estratégica, transforma a resposta a incidentes de um processo reativo para uma função inteligente, resiliente e proativa. Em vez de sobrecarregar os analistas com alertas constantes, capacita-os a focar no que realmente importa: investigar, aprender e adaptar-se a um cenário de ameaças em constante mutação.

A IT SECURITY É MEDIA PARTNER DO C-DAYS 2025

C-DAYS 2025: "UMA ENTIDADE QUE JÁ FAZ UMA GESTÃO MADURA NÃO TEM DE MUDAR O SEU MODUS OPERANDI COM A NIS2"

A REGULAÇÃO, E EM PARTICULAR A NIS2, FOI UM DOS TEMAS EM DESTAQUE NA EDIÇÃO DE 2025 DO C-DAYS, ORGANIZADO PELO CENTRO NACIONAL DE CIBERSEGURANÇA

RUI DAMIÃO

"+Resiliência" é o mote da edição de 2025 do C-Days. A conferência organizada pelo Centro Nacional de Cibersegurança (CNCS) voltou a ter lugar no Centro de Congressos do Estoril depois de uma edição em Coimbra (2024) e outra no Porto (2023). A IT Security é Media Partner do C-Days 2025.

Na sessão de abertura, Lino Santos, Coordenador do Centro Nacional de Cibersegurança, deu as boas-vindas aos presentes e partilhou que 38% das empresas em Portugal tem uma maturidade alta ou muito alta em resiliência, "mas também significa que temos um elevado número de empresas que não tem essa maturidade".

O volume de fraudes por meio digital continua a aumentar, assim como o ransomware. A inteligência artificial, diz Lino Santos, continua a crescer e são uma ameaça para as organizações e para os cidadãos. Também os computadores quânticos


LINO SANTOS, COORDENADOR DO CENTRO NACIONAL DE CIBERSEGURANÇA

colocam em causa a atual cibersegurança das organizações e é preciso preparar essa realidade.

Todas estes fatores trazem desafios para as organizações. "Afirmamos que a cibersegurança não é a segurança da informação. O que queremos proteger não é informação, mas sim a sociedade, o regime democrático. A cibersegurança existe para tornar a sociedade mais resiliente", afirma Lino Santos.

A transposição da NIS2, por exemplo, traz desafios, mas um conjunto de benefícios para as organizações, e para empresas de várias dimensões. "Precisamos de garantir o princípio da proporcionalidade", defende.

"Precisamos de apostar – e isto é uma grande oportunidade – na simplificação *by design*. Não vamos trazer nada de novo para as grandes empresas e ao seu *modus operandi*, mas podemos reduzir custos de contexto para a nossa economia", afirma.

Como desafios, há um claro aumento do número de organizações abrangidos pela NIS2 e é preciso "evitar a criação de uma regulamentação que tem como objetivo a conformidade", mas sim criar empresas verdadeiramente mais seguras.

Criar uma maior resiliência é "transmitir confiança aos cidadãos, parceiros de negócios e aos investidores de que Portugal é um país ciber-seguro", assim como ser "mais eficiente na alocação de recursos".

Pedro Brandão, Pró-Reitor da Universidade do Porto, que, em conjunto com o CNCS, organiza este C-Days, também afirmou que "as infraestruturas digitais são cada vez maiores e mais complexas. A informação é cada vez mais valiosa e as ameaças são cada vez mais sofisticadas", o que torna a cibersegurança num pilar essencial da sociedade.

"A cibersegurança tem de ser um estado de espírito" e "encarado como um pilar reputacional", refere Pedro Brandão. Com a presença no C-Days, a Universidade do Porto "procura conhecer as melhores práticas em cibersegurança", mas também "partilhar aquilo que temos vindo a aprender".

NIS2

O segundo dia do C-Days 2025 começou com uma sessão dedicada à NIS2 e aos instrumentos operacionais do Centro Nacional de Cibersegurança (CNCS). Lino Santos, Coordenador do CNCS, explicou que o objetivo é mostrar em que ponto é que a regulação está e qual é o *roadmap* para o futuro. "A regulação tem de permitir uma maior previsibilidade do que é esperado das organizações. O Regime Jurídico do Ciberespaço tem uma abordagem académica perfeita; no entanto, não traz previsibilidade. As organizações têm um vazio à sua frente e não sabem por onde começar ou avaliar os seus riscos", referiu.

O que o legislador tentou fazer com a transposição da NIS2 foi trazer essa previsibilidade. Depois de passos de autoquantificação, a organização consegue perceber que medidas tem de implementar. Após a transposição da NIS2, o regulamento terá de estar em consulta pública durante 30 dias – algo que o CNCS está pronto para que aconteça.

"Um segundo princípio é o da proporcionalidade. O mesmo regime jurídico tem de ser aplicado a empresas de grande dimensão – com grande experiência e maturidade – e a pequenas empresas – que ainda não têm essa experiência", afirma Lino Santos.

Por fim, o Coordenador do CNCS afirma que se procura a simplicidade por design. "O objetivo e aquilo que deve nortear o nosso trabalho é que haja uma coordenação entre autoridades competentes em cibersegurança e as autoridades setoriais para quando exigirmos uma determinada de cibersegurança estamos a cumprir com o regulamento NIS2 ou o regulamento do código da energia, por exemplo", explica Lino Santos.

"O objetivo é que haja uma plataforma que evite a duplicação da informação", refere o Coordenador, dando como exemplo o ataque à AMA em outubro, que obrigou a organização a comunicar junto de cinco entidades diferentes que tinha sofrido o ciberataque. Assim, o CNCS procura que as organizações tenham um trabalho mais simples e apenas tenha de notificar uma única entidade.

Atualmente, há dez países com implementação total da NIS2, sete de forma parcial e dez sem nenhum tipo de transposição. Assumindo que Portugal se inspira nas lições dos países que já implementaram, o modelo português segue o modelo belga.

Depois de se transpor a NIS2, será lançado um portal onde as entidades vão fazer a auto identificação de que são entidades reguladas. "A data em que esse portal é publicado serve de base para uma série de prazos: a partir daí, as entidades têm 60 dias para fazer o registo e é a data a partir do qual as organizações têm 24 meses para se adaptarem e estarem conforme a regulação". Quando acabar o prazo de auto identificação, as organizações vão saber todos os requisitos mínimos que têm de cumprir nos próximos 24 meses.

"O regulamento vai ter de contar com um novo quadro de referência para a cibersegurança – um processo que já realizamos – e não há é mais do que uma adaptação e atualização do Cybersecurity Framework do NIST", diz Lino Santos.

Este regulamento também precisa da definição daquilo que é a matriz de risco típica para cada setor – saúde, energia ou transportes. "Esse trabalho foi feito no primeiro trimestre deste ano e trabalhamos com comunidades ou associações setoriais para construir essas matrizes de risco", informa o Coordenador do CNCS.

"Uma entidade madura que já faz uma gestão madura não tem de mudar o seu *modus operandi*. Uma entidade nova que passa a ser alargada pelo regulamento, tem uma receita nova para seguir", explica. Deste modo, o CNCS "espera aumentar a resiliência e a segurança do país".

"Queremos fazer este caminho com as comunidades. O objetivo é ajudar-vos a crescer na maturidade de cibersegurança", conclui.

A IT SECURITY VIAJOU ATÉ FILADÉLFIA, NOS ESTADOS UNIDOS, A CONVITE DA AWS

AWS RE:INFORCE 2025: AS NOVAS FRONTEIRAS DA PROTEÇÃO DA CLOUD

DURANTE O RE:INFORCE 2025, A AWS APRESENTOU UM CONJUNTO DE NOVIDADES PARA A PROTEÇÃO DOS AMBIENTES CLOUD DAS ORGANIZAÇÕES E, EM ENTREVISTA, EXPLICOU COMO É QUE A CIBERSEGURANÇA EVOLUI.

RUI DAMIÃO

Amy Herzog, Vice-president e Chief Information Security Officer (CISO) da Amazon Web Services (AWS), subiu ao palco do AWS Re:Inforce 2025 – que se realizou em Filadélfia, nos Estados Unidos – para explicar como é que a AWS está a "simplificar a segurança em escala", para além de procurar mostrar como é que os serviços da AWS permitem contruir aplicações resilientes que conseguem "suportar as organizações frente às ameaças modernas", até porque, diz Herzog, "não podemos proteger adequadamente a Inteligência Artificial [IA] ou qualquer outra tecnologia sem uma base de segurança sólida". A IT Security viajou até Filadélfia a convite da AWS.

Herzog foi direta ao abordar os desafios atuais: "o ritmo das mudanças não está a diminuir. Nos próximos anos, vamos assistir a transformações rápidas, inúmeras

experiências e, inevitavelmente, alguns erros espetaculares pelo caminho". Esta realidade exige que as organizações repensem fundamentalmente as suas abordagens de segurança. "Às vezes pode parecer que a IA é como um estagiário rebelde que decide redesenhar todo o esquema da sua base de dados sem que ninguém o peça", afirmou a CISO da AWS, que espelha a tensão entre a inovação e o controlo que os CISO enfrentam diariamente.

GESTÃO DE IDENTIDADES E ACESSOS: A BASE

Em todo o mundo, a AWS processa 1,2 mil milhões de pedidos de API por segundo, o que demonstra a escala massiva da gestão de identidades moderna. Herzog enfatizou que "a identidade é sobre confiança; é sobre ter confiança suficiente para dizer que sabemos quem o utilizador é e, portanto, sabemos quem nós somos".

No evento, a AWS anunciou a disponibilidade geral do Internal Access Findings, uma nova capacidade do IAM Access Analyzer. Esta ferramenta utiliza raciocínio automatizado para mostrar exatamente que utilizadores têm acesso a recursos AWS importantes, como um S3 bucket, por exemplo.


AMY HERZOG, AMAZON WEB SERVICES (AWS)

A ferramenta analisa automaticamente vários tipos de políticas – identidade, recursos, políticas de controlo de serviços – e identifica quais as funções e utilizadores que têm acesso a recursos específicos. Ao mesmo tempo, o sistema verifica automaticamente as permissões de acesso todos os dias e pode notificar quando alguém novo obtém acesso a algo crítico.

SOBERANIA E PROTEÇÃO DE DADOS

A AWS implementou uma estratégia de defesa em profundidade ao nível da rede. Herzog explicou que o tráfego real na rede AWS mostra múltiplas camadas de encriptação. "É invulgar que o tráfego do cliente seja encriptado três ou mesmo mais vezes quando se move através da rede", partilha.

Outra novidade significativa é a capacidade de exportar certificados públicos emitidos pela ferramenta ACM e as suas chaves privadas para utilização dentro e fora da AWS. Esta funcionalidade permite que as organizações mantenham a gestão centralizada de certificados enquanto têm flexibilidade para usar os certificados onde for necessário.

A AWS também está a expandir as capacidades do AWS Shield com o lançamento do Network Security Director. Esta ferramenta realiza uma análise da rede, construindo uma topologia baseada nos recursos, conexões, serviços de segurança de rede e conjuntos de regras implementados.

Herzog anunciou, ainda, melhorias significativas no GuardDuty Extended Threat Detection, incluin-

do análises comportamentais avançadas, maior precisão com redução de falsos positivos, e nova cobertura para clusters EKS. Os resultados falam por si: num período de 90 dias, o GuardDuty Extended Threat Detection identificou mais de 13 mil sequências de ataque de alta confiança entre milhões de contas AWS monitorizadas.

Já o Security Hub aprimorado representa uma evolução fundamental na gestão de segurança na cloud. A plataforma combina sinais de segurança amplos e profundos de toda a AWS, correlacionando-os e enriquecendo-os para identificar e priorizar riscos ativos. A demonstração prática mostrou como o Security Hub pode combinar ameaças multiestágio detetadas pelo GuardDuty Extended Threat Detection com outros sinais, como vulnerabilidades, para priorizar questões críticas de segurança.

MODERNIZAÇÃO, AUTOMATIZAÇÃO E CORREÇÃO

A AWS introduziu, ainda, uma nova experiência de consola simplificada para o AWS WAF que reduz os passos necessários para configurar a segurança inicial da aplicação em 80%. Esta reimaginação da consola permite que as equipas de segurança protejam as suas aplicações em minutos em vez de horas.

Já a experiência de integração simplificada para o Amazon CloudFront permite que os programadores configurem uma solução abrangente que entrega conteúdo de forma rápida, segura e confiável, independentemente da sua experiência prévia.

Sobre as correções, Herzog afirmou que "o melhor *patching* é aquele que não se tem de fazer" e enfatizou a importância da modernização. A AWS oferece ferramentas especializadas para cada camada da *stack*: Amazon ECR scanning para *workloads* em *containers*, AWS Code Artifact para repositórios privados e Amazon Inspector para avaliação automática de aplicações.

Herzog concluiu ao dizer que o trabalho da AWS "não é abrandar a inovação; é garantir que todos nós possamos mover-nos ainda mais rapidamente". Para os CISO e diretores de cibersegurança, a mensagem é clara: a segurança eficaz na era da IA requer uma base sólida, ferramentas inteligentes e uma estratégia que equilibre proteção robusta com agilidade operacional.

AS COISAS BÁSICAS

Numa era em que se destacam diariamente ataques de ransomware sofisticados e ameaças de atores estatais, Mark Ryland, Director of Amazon Security, defende que o mais importante para a maioria das organizações é fazer o básico.

"A maioria dos ciberincidentes ocorre não devido a ataques sofisticados e complicados de alto nível, mas por coisas muito básicas, como sistemas sem correções ou emails de phishing", revelou contrariando o foco habitual dos diretores de cibersegurança em ameaças avançadas.

Esta realidade assume particular relevância em Portugal, onde, de acordo com os dados de 2023 da Pordata, 99,3% das empresas têm menos de 50 funcionários – organizações frequentemente sem recursos para equipas de segurança dedicadas, mas que podem beneficiar significativamente de abordagens pragmáticas aos fundamentos.

O PARADOXO DA PROCURA POR COMPLEXIDADE

Ryland admite frustração com uma tendência recorrente: "muito frequentemente os clientes dizem que querem ouvir mais sobre a mais recente evolução do cenário de ciberameaças, sobre quais são os mais recentes ciberataques incríveis que estão a acontecer". A resposta desafia esta mentalidade: "se fizer apenas o básico, provavelmente vai ficar bem". Para organizações com recursos limitados, esta perspetiva oferece uma abordagem mais sustentável que a corrida constante por soluções tecnológicas avançadas.


MARK RYLAND, AMAZON SECURITY

Mesmo sabendo que Mark Ryland trabalha num fornecedor de cloud específico, os princípios que partilha aplicam-se independentemente do fornecedor escolhido. Para as empresas mais pequenas, Ryland recomenda "escolher fornecedores de software com serviços reputados para que lhes forneçam os seus serviços de IT. Por outras palavras, não tentem gerir os vossos próprios servidores e bases de dados e websites", argumentando que "há uma riqueza de fornecedores muito capazes por aí".

Esta abordagem transfere complexidade técnica e responsabilidade de segurança para especialistas, permitindo que as organizações mais pequenas beneficiem de investimentos em segurança que individualmente não conseguiriam suportar.

Paralelamente, mantém-se a necessidade de formação básica dos colaboradores, especialmente relevante numa era em que a inteligência artificial generativa facilita a criação de "emails de phishing muito convincentes" em português correto, eliminando as pistas linguísticas que anteriormente ajudavam a identificar tentativas de fraude.

FALHAS DE ARQUITETURAS PERSISTENTES

Mesmo em ambientes cloud modernos, Ryland identifica duas vulnerabilidades recorrentes que revelam a persistência de problemas básicos: a autenticação multifator e as credenciais de longa duração.

Sobre o primeiro refere que "a falta de MFA é sempre um problema" e levou a AWS a adotar uma posição radical de, "literalmente, não permitir [ao cliente] fazer login até configurar o MFA" para contas privilegiadas.

Já sobre o segundo, o Director da AWS Security aconselha a "não utilizar credenciais de longa duração". O problema é estrutural: "estas credenciais, se forem de longa duração, tendem a andar por aí. São colocadas em código que não deviam". A migração para "credenciais temporárias" exige mudanças no processo, mas elimina uma categoria inteira de vulnerabilidades relacionadas com gestão inadequada da informação.

Mark Ryland destacou, também, uma capacidade específica da AWS, o Nitro, que diz ser algo que os CISO desconhecem e que oferece "um serviço de máquina virtual que não só protege de outros *tenants* num mundo *multi-tenant*, o chamado isolamento horizontal, como também protege de nós, do fornecedor cloud".

Esta proteção "não é uma funcionalidade adicional, não é algo extra pelo qual se pague", mas representa separação técnica fundamental: "não conse-

guimos ver o que se passa dentro da computação, armazenamento e bases de dados quando usam esta tecnologia".

Para os responsáveis de cibersegurança preocupados com dependência excessiva de fornecedores cloud, esta separação arquitetural oferece garantias técnicas além de contratuais. Para além da AWS, também a Google Cloud e a Microsoft Azure disponibilizam serviços semelhantes para computação confidencial.

COLABORADORES COMO PRIMEIRA LINHA DE DEFESA

A Amazon adota o princípio de "ver algo, dizer algo" através da cultura organizacional que encoraja o reporte sem penalizações. "Preferimos muito mais ouvir de todos os nossos funcionários e clientes, qualquer pessoa, que acham que algo está errado, mesmo que acabe por ser um falso positivo", afirma.

A lógica é simples: os colaboradores "notam coisas mais frequentemente do que a equipa de cibersegurança, que não tem visibilidade sobre tudo o que é utilizado no dia a dia da operação".

O resultado são "muitos falsos positivos, sim, mas, em geral, isso vai realmente ajudar uma empresa a elevar o seu nível". Para organizações sem recursos para monitorização 24/7, esta abordagem oferece capacidades de deteção distribuídas – ainda que limitadas – sem investimento tecnológico significativo.

TRANSPARÊNCIA COMO DIFERENCIAÇÃO

Questionado sobre uma eventual relutância organizacional em discutir cibersegurança, Ryland propõe uma mudança de perspetiva: admitir imperfeições pode constituir uma vantagem competitiva ao "construir confiança na base de clientes" através da transparência. Esta abordagem torna-se mais relevante com regulamentação como NIS2, que exige divulgação de incidentes significativos.

A perspetiva de Mark Ryland sugere que a execução rigorosa de fundamentos oferece proteção eficaz para a maioria das organizações. Para os diretores de cibersegurança em empresas portuguesas – especialmente com menos de 50 colaboradores – esta abordagem oferece um caminho sustentável para melhorar a postura de segurança com recursos limitados.

A chave está em reconhecer que "se fizer apenas o básico, provavelmente vai ficar bem" – uma perspetiva que pode transformar estratégias de gestão de risco baseadas em fundamentos sólidos em vez de corridas tecnológicas insustentáveis. ◀

A IT SECURITY EM MADRID, ESPANHA, A CONVITE DA KASPERSKY

O HORIZONTE DIGITAL:
IA, QUANTUM E O FUTURO DA CIBERSEGURANÇA

A INTELIGÊNCIA ARTIFICIAL E A COMPUTAÇÃO QUÂNTICA DOMINARAM O KASPERSKY HORIZONS, EM MADRID, ONDE ESPECIALISTAS ALERTARAM PARA A CRESCENTE SOFISTICAÇÃO DO CIBERCRIME. ENTRE ÉTICA, RESILIÊNCIA E NOVOS RISCOS, O EVENTO DEIXOU CLARO QUE O FUTURO DA CIBERSEGURANÇA EXIGE REPENSAR ESTRATÉGIAS.

INÊS GARCIA MARTINS

Madrid foi palco do Kaspersky HORIZONS, num dia dedicado aos desafios emergentes da cibersegurança, num cenário cada vez mais impactado pela Inteligência Artificial (IA) e pela computação quântica. O Riu Plaza Hotel foi o epicentro deste encontro internacional que reuniu profissionais de diversas geografias e áreas que atuam na linha da frente, desde o *hacking* ético à investigação avançada de ameaças. A IT Security marcou presença no evento a convite da Kaspersky.

"A IA está a desafiar e a transformar todas as indústrias, inclusive a própria cibersegurança", afirmou Óscar Suela, General Manager Iberia da Kaspersky, na sessão de abertura. O responsável defendeu a necessidade de repensar estratégias de defesa e lançou um alerta para o futuro próximo, em que "não falaremos apenas de zeros e uns, mas também de qubits".

"Os cibercriminosos são, hoje, o sistema imunitário da internet", afirmou Clément Domingo no primeiro *keynote* do dia, onde traçou um retrato direto da realidade no terreno. O Ethical Hacker e Cybersecurity Evangelist alertou para a atividade de mais de 200 grupos, dos quais 40 estão muito ativos e dez são "extremamente perigosos", com operações globais. Através do exemplo de uma investigação que expôs as rotinas internas de um grupo de ransomware – desde a escolha dos alvos às táticas usadas, passando pelos jantares em restaurantes com estrela Michelin como forma de celebração – destacou como a Inteligência Artificial está a acelerar e sofisticar os ataques, permitindo automatizar processos que antes levavam semanas.

Jochen Michels, Head of Public Affairs Europe da Kaspersky, defendeu a importância da cooperação *multistakeholder* para construir uma IA ética e fortalecer a ciberresiliência. "Só teremos sucesso na luta contra o cibercrime se o lado do bem trabalhar tão bem em conjunto como o lado do mal trabalha", afirmou, referindo-se a iniciativas como o projeto NoMoreRansom ou a coligação contra o Stalkerware. Apresentou ainda os princípios que devem guiar o uso da IA em cibersegurança, desde a transparência – "os utilizadores devem saber quando e como a IA é usada" – até ao respeito pela privacidade, passando pelo controlo humano, segurança desde a origem e compromisso exclusivo com fins defensivos.

ÓSCAR SUELA, KASPERSKY


CLÉMENT DOMINGO, ETHICAL HACKER E CYBERSECURITY EVANGELIST

Na mesa-redonda "*Responsible AI: Challenges, Choices and Change*", Liliana Acosta, Founder e CEO da Thinker Soul, alertou para a "erosão da autonomia das pessoas" causada pela concentração de poder nas grandes tecnológicas e defendeu que a ética exige "pensar antes de agir". Clément Domingo lembrou que "IA não é o ChatGPT" e sublinhou a necessidade de combater visões simplistas e garantir segurança e compreensão por parte dos utilizadores. Já Marc Rivero, Lead Security Researcher na Kaspersky, expressou preocupação com o desconhecimento sobre o impacto futuro da IA e destacou o centro de transparência da empresa como exemplo de construção de confiança.

Marc Rivero manteve-se em palco para apresentar as conclusões de um relatório privado sobre uma nova geração de ransomware. "Os cibercriminosos estão a usar a IA para criar e-mails de phishing perfeitos, automatizar campanhas e gerar *scripts* que exploram palavras-passe esquecidas", alertou. Destacou o FunkSet, um ransomware em VASC, compilável para várias arquiteturas, que num único binário cifra ficheiros e exfiltra dados. Sublinhou ainda que o grupo por trás do FunkSet distribui parte do código-fonte para recrutar afiliados, tornando o crime

MESA-REDONDA "RESPONSIBLE AI: CHALLENGES, CHOICES AND CHANGE"


MARC RIVERO, KASPERSKY

mais acessível. "A inteligência artificial não está só a fortalecer a defesa, é também uma força multiplicadora para os atacantes", concluiu.

AUTOMATIZAÇÃO DE ATAQUES E ALGORITMOS PÓS-QUÂNTICOS NO CENTRO DAS PREOCUPAÇÕES

Sergey Lozhkin, Head of APAC & META Research Centers da Kaspersky GReAT, analisou o impacto da computação quântica na cibersegurança, salientando que "não é preciso saber como funciona um processador quântico para perceber o risco". Apesar dos avanços da Google ou da IBM, garantiu que "os computadores quânticos ainda não conseguem quebrar algoritmos como o RSA, pois seriam necessários milhões de qubits sem erros". Advertiu, no entanto, que, "talvez em dez ou 15 anos, ou até antes, governos possam usar estes sistemas para ciberespionagem" e defendeu que a migração para algoritmos pós-quânticos será uma necessidade, algo que "veremos com grande pressão nos próximos anos".

No debate "*Hope vs Hype – How will Quantum Computing Change the Cyber Security World?*", discutiu-se o impacto real da computação quântica na cibersegurança. "Com cada qubit adicional, duplicamos exponencialmente a capacidade de processamento", explicou Johannes Verst, CEO e fundador da Quantum Business Network, destacando o potencial disruptivo da tecnologia. Nas palavras de Pilar Troncoso, Chief Relations Officer da QCentroid, "não é apenas mudar procedimentos, é mudar a forma como pensamos e experimentamos a tecnologia", realçando a necessidade de preparar as empresas para a mudança. Já Sergey Lozhkin alertou que "só quando o desastre acontece é que as empresas começam a agir – mas na cibersegurança, esse atraso pode ser fatal". Embora o computador quântico universal ainda esteja longe, o consenso é planear, educar e testar já para evitar prejuízos futuros.

VISÃO DOS ESPECIALISTAS: COLABORAÇÃO, IA E ENGENHARIA REVERSA

À conversa com a IT Security, Marc Rivero apontou os principais desafios da cibersegurança, especialmente com a IA a aumentar a complexidade do crime digital. Destacou problemas como a exposição de serviços externos e a falta de atualizações, sendo que "as pessoas esquecem-se de atualizar o software, o que significa que o sistema fica vulnerável". Também alertou para falhas dos utilizadores que "não configuram a autenticação de dois fatores, não mudam as palavras-passe regularmente e utilizam informações corporativas fora da organização". A IA confere aos criminosos capacidades inéditas, tornando-os "praticamente especialistas em tudo", incluindo phishing e malware. Para dar resposta a esses incidentes, a palavra de ordem para Marc Rivero é a colaboração e reforçou que "não conseguimos sobreviver, do ponto de vista da defesa, se não partilharmos o que observamos". "Sem colaboração entre o público e o setor privado, não conseguimos fazer nada contra os '*bad guys*'", sublinhando a importância de os CISO conhecerem as técnicas usadas para aplicar defesas, lembrando que "as TTP continuam lá" apesar das mudanças nas redes. Para o Lead Security Researcher na Kaspersky, a partilha de informação é essencial para acompanhar a evolução das ameaças.

SERGEY LOZHKIN, KASPERSKY GREAT

Por sua vez, Sergey Lozhkin avisou que os CISO devem preparar-se para as ameaças futuras, em particular o uso de IA por grupos APT. O Head of APAC & META Research Centers da Kaspersky GReAT salientou que "cada CISO não só deve compreender a minha experiência, mas qualquer experiência ligada à cibersegurança" e que "os CISO precisam mesmo de estar a par das ameaças futuras". Além disso, explicou que o cibercrime financeiro está a migrar para as criptomoedas, o que facilita ataques de grupos como o Lazarus, que usam técnicas sofisticadas como "zero-days, exploração de vulnerabilidades" e "*payloads* maliciosos, *backdoors*". O especialista destacou a engenharia reversa como essencial para detetar APT, e afirmou que "a competência técnica mais avançada, a mais indispensável, é sem dúvida a capacidade de fazer engenharia reversa". A inteligência artificial é, para Sergey Lozhkin, o fator que veio aumentar a sua produtividade para "cinco, dez vezes" mais, ao acelerar a análise de código. Sobre o quantum, disse que "não é algo para agora", mas que pode facilitar "quebrar encriptação" no futuro. Por isso, alertou que "os CISO não devem estar totalmente tranquilos ao pensar na utilização de IA em ataques APT" e devem "começar a informar-se sobre isso já" para não ficarem expostos.

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:
Beatriz Salzedas - (+351) 910 788 082 - beatriz.salzedas@medianext.pt
João Calvão - (+351) 910 788 413 - joao.calvao@medianext.pt
MARKETING & EVENTS DIRECTOR:
Rosa Bento - rosa.bento@medianext.pt
MARKETING COMMUNICATIONS:
Rita Rodrigues - (+351) 912 971 161 - rita.rodrigues@medianext.pt
ARTE E PAGINAÇÃO: Teresa Rodrigues
DESENVOLVIMENTO WEB: Global Pixel

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

IT Insight Security é membro de:

ASSOCIAÇÃO PORTUGUESA DE IMPRENSA · ACEPI ASSOCIAÇÃO ECONOMIA DIGITAL · CIWA COMPETITIVE INTELLIGENCE & INFORMATION WARFARE ASSOCIATION

Editado por:

media NEXT
STAY AHEAD • STAY RELEVANT