CIBERSEGURANÇA

APOIOS:

CELFOCUS

MEO EMPRESAS

SIBS CyberWatch

ZURICH

ENQUADRAMENTO

NOVOS RISCOS NA CIBERSEGURANÇA NACIONAL

PORTUGAL DESTACA-SE ENTRE OS PAÍSES MAIS AVANÇADOS EM CIBERSEGURANÇA, MAS ENFRENTA UM AUMENTO EXPRESSIVO DE INCIDENTES

O nosso país apresenta, neste momento, um retrato duplo no domínio da cibersegurança. De um lado, os dados mais recentes do Centro Nacional de Cibersegurança (CNCS) revelam um aumento significativo do número de incidentes registados; do outro, o País alcança uma das melhores classificações mundiais no Global Cybersecurity Index 2024, da União Internacional das Telecomunicações, que avalia a maturidade e a capacidade de resposta dos Estados nesta área.

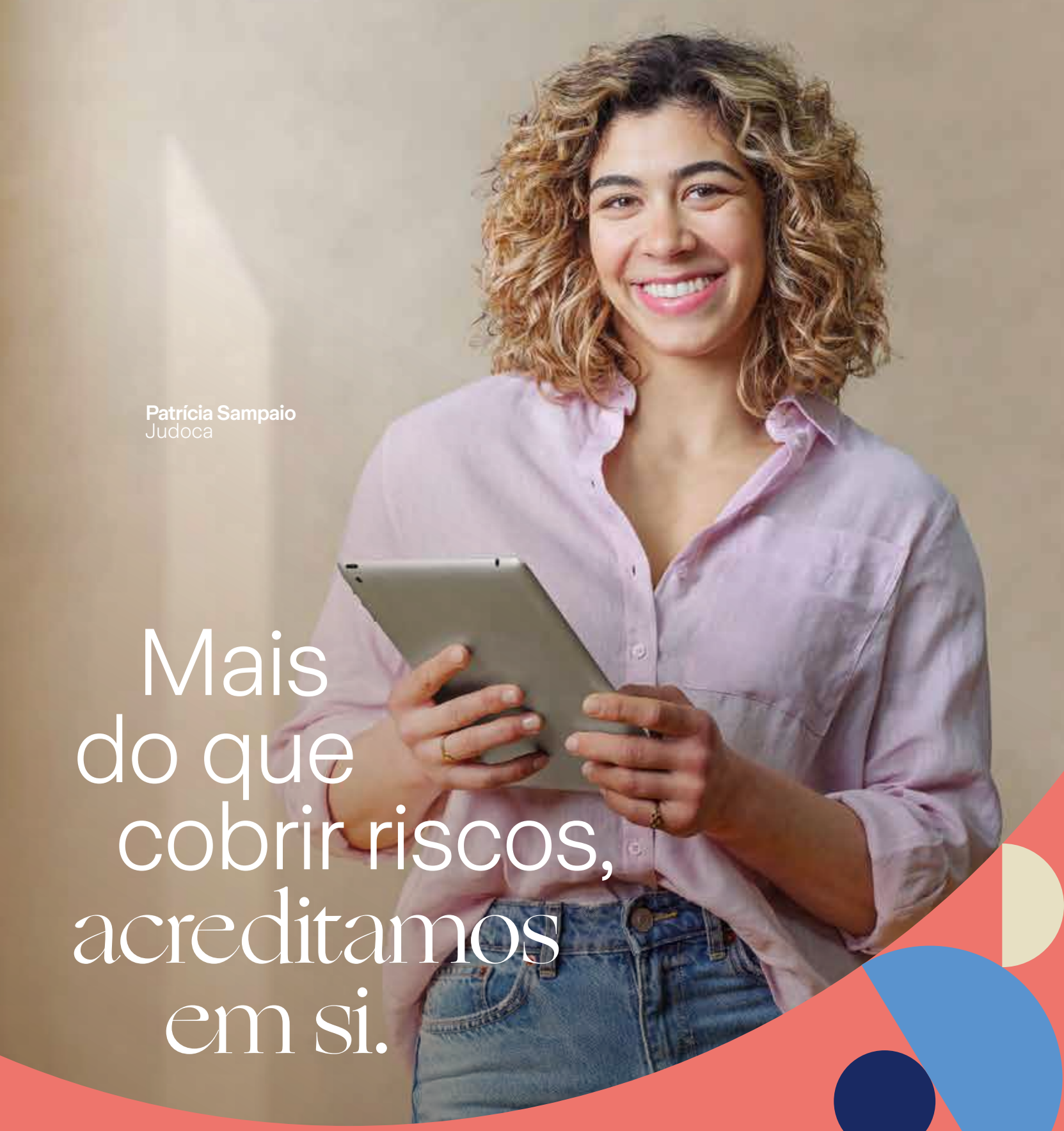
De acordo com o relatório «Riscos & Conflitos», divulgado pelo CNCS, o número de incidentes de cibersegurança comunicados ao CERT.PT subiu 36% em 2024 face ao ano anterior, totalizando 2758 ocorrências. Cerca de 78% desses casos envolveram entidades privadas, sendo o sector público responsável pela parte restante. A maioria dos incidentes corresponde a ataques de phishing e smishing, que voltaram a ser os mais frequentes, registando um crescimento de 13%. A engenharia social foi a tipologia que mais aumentou, passando a ocupar o segundo lugar entre as ameaças mais reportadas.

Entre os episódios com impacto mais elevado, destacaram-se ataques de ransomware, falhas críticas que causaram interrupções de serviço e casos de roubo ou fuga de credenciais pertencentes a entidades públicas, operadores de serviços essenciais e prestadores de serviços digitais. O relatório assinala também novas formas de fraude, como o vishing, o CEO fraud, o falso recrutamento e as burlas conhecidas por "Olá, Pai" ou "Olá, Mãe". O crescimento foi particularmente notório nos sectores e áreas governativas da energia e da administração pública local e regional. Já o sector bancário apresentou uma redução de cerca de 69% no número de incidentes e deixou de figurar entre os mais atingidos, passando do terceiro lugar em 2023 para o nono em 2024.

NOTA (QUASE) MÁXIMA

Em paralelo com esta evolução, Portugal obteve uma pontuação quase perfeita no Global Cybersecurity Index 2024, atingindo 99,86 pontos em 100 possíveis, acima dos 97,32 registados em 2021. O País integra agora o grupo de referência da UIT – o Tier 1 – que reúne as nações consideradas modelo em maturidade e capacidade no domínio da cibersegurança. A avaliação teve em conta vários factores, incluindo o enquadramento jurídico, os mecanismos técnicos e organizacionais, o desenvolvimento de competências e a cooperação internacional.

A conjugação destes dois retratos – o aumento expressivo dos incidentes e a classificação de topo a nível internacional – espelha um contexto em que as capacidades técnicas e institucionais coexistem com uma crescente pressão operacional. O reconhecimento internacional confirma o avanço das políticas e estruturas de segurança digital, enquanto os dados nacionais mostram que as ameaças continuam a evoluir em número e sofisticação. ●



Patrícia Sampaio
Judoca

Mais do que cobrir riscos, acreditamos em si.

Consulte um mediador Zurich, aceda à App Z4U ou visite-nos em zurich.com.pt.

Para que tudo corra bem.

Esta informação é da responsabilidade da **Zurich Insurance Europe AG, Sucursal em Portugal** e da **Zurich – Companhia de Seguros Vida, S.A.**, registadas na ASF sob os números 1184 e 1132 respetivamente. **Esta publicidade não dispensa a consulta da informação pré-contratual e contratual legalmente exigida, disponível em zurich.com.pt, na App Z4U e em qualquer mediador Zurich.**

ZURICH®

CELFOCUS

DESENVOLVER INTELIGÊNCIA ARTIFICIAL SEGURA: PRÁTICAS ESSENCIAIS

A INTELIGÊNCIA ARTIFICIAL ESTÁ CADA VEZ MAIS INTEGRADA EM PRODUTOS E SERVIÇOS, EXIGINDO ATENÇÃO À SEGURANÇA, FIABILIDADE E ÉTICA DESDE O DESIGN ATÉ À OPERAÇÃO

Nos últimos anos, a Inteligência Artificial (IA) deixou de ser um tema exclusivo do mundo académico ou de empresas altamente especializadas e passou a integrar produtos e serviços do dia a dia, como assistentes virtuais, tradutores ou sistemas de recomendação.

Em entrevista à Executive Digest, Pedro Tarrinho, director of Application Security da Celfocus, explica de que forma a segurança, a fiabilidade e a ética devem estar presentes em todas as fases do desenvolvimento de soluções de IA, desde o design até à monitorização contínua, e os desafios que as empresas enfrentam para garantir que estas tecnologias são seguras, transparentes e responsáveis.

Quando e como é que conceitos como ML e NLP começaram a ganhar relevância no desenvolvimento de soluções de IA?

Embora actualmente se fale muito

em IA, a verdade é que conceitos como ML e NLP já são estudados há várias décadas. Acontece que até há poucos anos estavam mais confinados ao mundo académico ou a empresas muito especializadas. Na minha opinião, o ponto de viragem foi a capacidade de treinar modelos com grande volume de dados e a evolução do hardware/computadores. Isto permitiu que estes conceitos começassem a ser usados em produtos reais, como assistentes virtuais, tradutores, sistemas de análise de imagens, etc, e, mais recentemente, com os modelos generativos, que trouxeram tudo isto para o dia a dia das empresas e das pessoas.

Ao falar de usar IA em soluções empresariais, o que é que isso implica na prática em termos de segurança e fiabilidade?

Aqui é importante separar duas realidades diferentes. Por um lado, temos os programadores que usam IA como ferramenta de apoio, para escrever código, gerar testes, rever documentação, etc, e isso, apesar de parecer inofensivo, também traz riscos. O código gerado nem sempre é seguro, pode ter erros escondidos (propositados) ou usar formas de fazer as coisas que já não são recomendadas. É preciso validar tudo, não confiar cegamente. No desenvolvimento assistido por IA, a regra é clara: o responsável pelo código é o humano e não o Large Language Model.

Depois há o outro lado: quando a IA faz parte da solução final, como um chatbot, num sistema de recomendação ou num agente

» Pedro Tarrinho, director of Application Security da Celfocus

inteligente. Aqui o desafio aumenta porque deixamos de ter apenas uma ferramenta de apoio e passamos a ter uma "entidade" que interage com utilizadores, aprende com dados e toma decisões com impacto real. Isso implica garantir que esse sistema IA é fiável, que não revela informação sensível, que não pode ser manipulado com inputs maliciosos e que se comporta de forma previsível. A segurança tem de ser pensada do início até ao fim.

O que significa exactamente desenvolver IA de forma segura? É diferente do desenvolvimento seguro de software tradicional?

É diferente, sim. Com o software tradicional, lidamos com lógica e regras que conhecemos desde o início. Com a IA, existe um grau de imprevisibilidade: os modelos aprendem, ajustam-se, podem tomar decisões influenciadas por regras que nem sempre percebemos e reagir de forma inesperada. Desenvolver IA de forma segura significa controlar melhor os dados de input e perceber bem como o modelo aprende, de forma a garantir que há limites bem definidos para o que ele pode ou não fazer. É pensar na segurança como algo contínuo e não apenas como uma fase final, o famoso Shitf Left, mas de IA.

«DEPOIS DE UM SISTEMA DE IA ENTRAR EM PRODUÇÃO, NÃO É POSSÍVEL ASSUMIR QUE O COMPORTAMENTO DEFINIDO INICIALMENTE VAI CONTINUAR ESTÁVEL E SEM SOBRESSALTOS»

Como é que a vossa abordagem garante que a segurança está presente desde o design das soluções de IA?

Este é um tema no qual temos vindo a trabalhar há bastante tempo. Investigamos e testamos formas de integrar segurança logo desde o início, e isso levou-nos a criar um processo interno muito claro e adaptado à realidade de IA. Esse processo cobre todas as fases do ciclo de vida, desde o planeamento até à monitorização. Para nós, a "segurança desde o design" não é só uma ideia bonita, é algo que fazemos na prática, com base num processo bem definido.

Que práticas aplicam ao longo do ciclo de vida da IA para prevenir riscos éticos e evitar enviesamentos nos modelos?

Temos vindo a construir um processo que acompanha todas as fases do desenvolvimento, desde o planeamento até à operação. Logo no início do projecto de desenvolvimento, analisamos os dados com que vamos trabalhar para garantir

que não introduzem tendências ou desequilíbrios que possam influenciar o comportamento do modelo. Mais à frente, quando o modelo está a ser treinado, fazemos testes para perceber se responde de forma consistente e adequada a diferentes situações e perfis de utilizador. Ao longo do processo, envolvemos pessoas de várias áreas (técnica, jurídico e de negócio) para trazer diferentes perspectivas e identificar potenciais impactos que podem não ser sempre óbvios.

De que forma validam e testam a segurança e a resiliência dos modelos antes da sua implementação?

Antes de passar a produção, qualquer modelo passa por uma fase de testes que tenta replicar tanto o uso normal como situações fora da "caixa". Simulamos interacções maliciosas, testamos comportamentos com diferentes tipos de inputs e tentamos perceber até que ponto o modelo se consegue manter estável e seguro. Também avaliamos se há risco de "data leak" que devia estar protegida e se há falhas na forma como o modelo lida com pedidos mais sensíveis. Não existe um sistema 100% seguro, mas os testes que efectuamos têm como objectivo reduzir ao máximo o risco antes de chegarem às mãos dos utilizadores finais.

Como garantem que os dados utilizados são tratados de forma segura e em conformidade com o GDPR e outras normas europeias?

No início de cada projecto fazemos um mapeamento dos dados que vamos usar e avaliamos se estão a ser tratados de forma correcta e com base legal. Nesta fase, identificamos as medidas que serão aplicadas: anonimização, remoção, encriptação, entre outras. As regras de retenção e a forma como os dados "circulam" fazem parte do nosso processo. Este trabalho inicial pode prolongar a fase de arranque, mas é um investimento que evita riscos futuros e, sobretudo, aumenta a confiança de quem vai utilizar a solução.

Que papel desempenha a monitorização contínua na manutenção da segurança e da confiança operacional dos sistemas de IA?

É uma das fases mais críticas na nossa abordagem. Depois de um sistema entrar em produção, não é possível assumir que o comportamento definido inicialmente vai continuar estável e sem sobressaltos. A realidade muda, os utilizadores mudam, os mecanismos de ataque mudam, por isso a monitorização contínua permite detectar problemas mais cedo, seja por uma quebra de desempenho, respostas erradas, ou até sinais de uso malicioso. No final do dia, é o que nos permite ter visibilidade se a IA continua a comportar-se como esperado.

De que forma a ética e a transparência nos modelos de IA contribuem para a confiança dos utilizadores e clientes?

As pessoas não confiam em sistemas que não compreendem. O carácter não determinístico da IA, o facto de não dar sempre a mesma resposta, acrescenta complexidade e pode gerar desconfiança.

«NO INÍCIO DE CADA PROJECTO FAZEMOS UM MAPEAMENTO DOS DADOS QUE VAMOS USAR E AVALIAMOS SE ESTÃO A SER TRATADOS DE FORMA CORRECTA E COM BASE LEGAL»

É aqui que a transparência faz a diferença: explicar o que está por detrás das respostas, deixar claros os limites dos sistemas e garantir que as decisões não são tomadas de forma cega. As soluções de IA

«NO MOMENTO EM QUE BAIXAMOS A GUARDA, CORREMOS O RISCO DE PERDER O CONTROLO»

têm de ser desenhadas desde o início com clareza, previsibilidade e princípios éticos. Só assim será possível construir confiança e credibilidade junto de utilizadores e clientes.

Quais são os principais desafios que as empresas enfrentam ao tentar cumprir o AI Act e outros requisitos regulatórios?

Um dos primeiros desafios é perceber o que realmente se aplica ao que se está a desenvolver. O AI Act é um regulamento europeu, o que significa que se aplica a todos os países da EU. No entanto, como aconteceu com o RGPD, e não sendo eu da área jurídica, acredito que cada país tenha de o ajustar à sua legislação.

» «Logo no início do projecto de desenvolvimento, analisamos os dados com que vamos trabalhar para garantir que não introduzem tendências ou desequilíbrios que possam influenciar o comportamento do modelo»

Depois, há o desafio prático, que é gerir e documentar o ciclo de vida de um projecto IA, desde avaliar riscos, garantir a transparência (explicabilidade), gerir dados sensíveis, etc. Há que garantir uma abordagem transversal com as equipas certas, desde segurança, jurídica, compliance, produto, tecnologia, etc.

Por fim, a classificação por níveis de risco. Desde os mais elevados, como saúde, justiça ou infraestruturas críticas, que exigem regras muito mais rigorosas, até aos sistemas de IA de risco limitado, usados apenas para interpretar documentos ou apoiar processos. Esta diferenciação é um ponto essencial que deve ser analisado e considerado à luz do AI Act.

Que erros ou lacunas observam frequentemente quando soluções de IA são desenvolvidas sem segurança embutida desde o início?

As mais comuns são soluções que funcionam tecnicamente, mas que falham em aspectos críticos, porque os modelos não foram devidamente testados para perceber como reagem a inputs inesperados, não têm mecanismos para detectar se estão a revelar informação sensível ou a tomar decisões incoerentes. Também é frequente haver falta de controlo dos dados usados, desde a sua origem até ao impacto no comportamento do sistema final. Se tivemos a segurança em mente, conseguimos analisar as decisões tomadas e garantir explicações e, com isso, reforçar a confiança, reduzir riscos a longo prazo, aumentando, assim, a segurança.

Olhando para o futuro, que passos considera essenciais para que a IA continue a ser segura, confiável e responsável?

O mais importante é continuarmos a olhar para a AI com senso crítico e não deslumbramento e medo. A tecnologia vai evoluir, os modelos vão ficar mais capazes, mas o essencial não muda: temos de garantir que o que estamos a construir é seguro, transparente e resiliente. Isto implica manter processos claros, envolver pessoas com diferentes perfectivas e nunca tratar a segurança como um extra. Por fim, temos de manter a humildade.

No dia em que acreditarmos que já compreendemos a IA por completo, será provavelmente o início do fim. O momento em que baixamos a guarda, corremos o risco de perder o controlo. ●

MEO EMPRESAS

A SEGURANÇA DIGITAL EM PRIMEIRO LUGAR

A MEO TEM REFORÇADO A ÁREA DA CIBERSEGURANÇA COM TECNOLOGIAS AVANÇADAS, GARANTINDO A PROTECÇÃO DE REDES E EMPRESAS PERANTE O AUMENTO DAS AMEAÇAS DIGITAIS

Face à crescente complexidade e sofisticação das ameaças digitais, a MEO tem investido continuamente em soluções e tecnologias que permitem antecipar, detectar e neutralizar ataques, garantindo a resiliência das suas redes e a protecção dos seus clientes. Em entrevista à Executive Digest, Pedro Inácio, CISO e director de Cybersecurity & Privacy da MEO, destaca a importância da cibersegurança no cenário actual, revelando qual a estratégia da empresa para combater os ataques digitais, os investimentos em inovação e os desafios de proteger infra-estruturas críticas e clientes empresariais.

A cibersegurança é hoje uma preocupação central para qualquer organização. Como é que uma empresa de telecomunicações como a MEO garante a resiliência da sua rede perante o aumento das ameaças digitais?

Na MEO olhamos para a cibersegurança como um pilar essencial da nossa actividade. É o que garante a continuidade dos serviços que prestamos a milhões de clientes todos os dias. Temos uma rede de fibra óptica de última geração e uma rede móvel de alta qualidade, com cobertura nacional, dotadas de robustos esquemas de redundância. O nosso Cyber Security Operations Center (CyberSOC), que opera 24 horas por dia, permite-nos monitorizar milhares de eventos, utilizando

tecnologias de referência. Isso permite-nos detectar e neutralizar ameaças em fases iniciais, garantindo que os serviços não são afectados mesmo perante ataques complexos.

Que tipo de investimentos estruturais têm vindo a ser feitos pela MEO para proteger clientes empresariais na área da cibersegurança?

Temos feito investimentos consistentes em soluções consideradas "best of breed" no mercado, como ferramentas SIEM (Security Information and Event Management), SOAR (Security Orchestration, Automation and Response) e plataformas de threat intelligence. Estes sistemas dão-nos maior capacidade de análise e resposta proactiva. Além disso, criámos a unidade de Cyber Warfare Operations (CWO), que disponibiliza serviços geridos de segurança. O objetivo é simples: permitir que os nossos clientes empresariais se concentrem no seu negócio, enquanto asseguramos a protecção do seu ambiente digital. Esse trabalho foi reconhecido em 2025, aquando da conquista do prémio de Melhor Gestor de Segurança da EMEA, atribuído pela Rapid7.

As PME são frequentemente alvos fáceis de ataques. Que soluções disponibiliza a MEO para ajudar estas empresas que muitas vezes não têm equipas próprias de IT?

As PME são, de facto, mais vulneráveis, porque nem sempre dispõem de equipas internas de IT. Pensando nisso, desenvolvemos uma oferta adaptada: soluções de anti-DDoS (Anti Distributed Denial of Service), VPN seguras, backups na cloud e firewalls avançadas, sempre com acompanhamento personalizado. Oferecemos também gestão partilhada de segurança, o que significa que as PME conseguem ter acesso a tecnologias de ponta e a suporte especializado sem necessidade de criar estruturas internas próprias.

A transformação digital acelerou a migração de processos para a Cloud. Que papel desempenha a MEO na proteção dos dados e aplicações que circulam nas suas plataformas?

A protecção dos dados é para nós uma prioridade máxima. Nos nossos data centers e nas plataformas cloud que operamos, aplicamos auditorias automáticas, monitorização contínua e políticas de segurança ajustadas à evolução do mercado. Tudo isto faz parte da nossa Doutrina Activa de Cibersegurança, que abrange desde a prevenção e protecção até à recuperação activa, garantindo que as aplicações e os dados circulam de forma segura e com total integridade.

ESTRATÉGIA A CIBERSEGURANÇA É VISTA PELA MEO COMO UM PILAR ESTRATÉGICO DA SUA ACTIVIDADE, ASSEGURANDO A CONTINUIDADE DOS SEUS SERVIÇOS QUE PRESTAM DIARIAMENTE A MILHÕES DE CLIENTES

O ransomware tornou-se uma das maiores ameaças actuais. Que medidas podem as empresas adoptar em conjunto com a MEO para mitigar este risco?

O ransomware só pode ser combatido com uma abordagem conjunta. Do nosso lado, disponibilizamos backups seguros na cloud, monitorização avançada para detecção precoce e programas de sensibilização e formação. O nosso CyberSOC é também uma peça-chave, pois garante resposta imediata e minimiza impactos. Mas a cooperação com os clientes é fundamental, porque a cibersegurança começa sempre dentro das organizações.

Em termos de monitorização, como a MEO consegue identificar e responder rapidamente a incidentes de segurança em larga escala?

No CyberSOC da MEO analisamos diariamente milhares de potenciais incidentes. Os sistemas de automação tratam grande parte deles, mas os mais críticos são escalados para equipas especializadas que actuam de forma rápida e coordenada. Além disso, estamos ligados a redes nacionais e internacionais de CERTs (Computer Emergency Response Teams) e cooperamos com entidades como a NATO e a Europol, o que nos dá uma visão global e fortalece a nossa capacidade de resposta.

Muitos gestores preocupam-se com a confidencialidade das comunicações. Que garantias pode

» «O nosso Cyber Security Operations Center (CyberSOC), que opera 24 horas por dia, permite-nos monitorizar milhares de eventos, utilizando tecnologias de referência»

a MEO dar sobre a protecção do tráfego de voz e dados?

A protecção da privacidade é central na política de segurança da MEO. Mantemos certificações como a ISO 27001 (Segurança da Informação) e ISO22301 (Continuidade do Negócio) e aplicamos práticas de segurança em profundidade. As comunicações de voz e dados são encriptadas e monitorizadas em permanência. Os nossos clientes podem confiar que a sua informação é tratada com o mais alto nível de protecção.

Que papel tem a colaboração da MEO com entidades públicas e outras operadoras no reforço da cibersegurança nacional?

A cibersegurança não se garante de forma isolada. Trabalhamos em conjunto com o governo, reguladores, como é o caso do Centro Nacional de Cibersegurança e outros operadores, para proteger infra-estruturas críticas. Participamos em exercícios conjuntos, como o CyberEurope e o Cascade, e estamos integrados em redes europeias de CERTs, o que nos permite partilhar informação e alinhar estratégias. É esse trabalho colaborativo que reforça a segurança nacional.

A inteligência artificial e a análise avançada de dados são cada vez mais usadas na prevenção de ataques. A MEO já integra estas ferramentas nas suas operações?

Sem dúvida. A MEO está na linha da frente na utilização de inteligência artificial em cibersegurança. Trabalhamos com algoritmos que permitem detectar padrões anómalos, detectar precocemente ataques e até automatizar respostas. Estas tecnologias tornam-nos mais rápidos e mais eficazes.

«DESDE 2020, TODOS OS NOSSOS UTILIZADORES SÃO ALVO DE CAMPANHAS SIMULADAS DE PHISHING E TÊM FORMAÇÃO CONTÍNUA, O QUE AJUDA À ADOPÇÃO DE BOAS PRÁTICAS DE SEGURANÇA NO SEU DIA-A-DIA»

Que desafios encontra a MEO na sensibilização e formação dos clientes empresariais para práticas seguras?

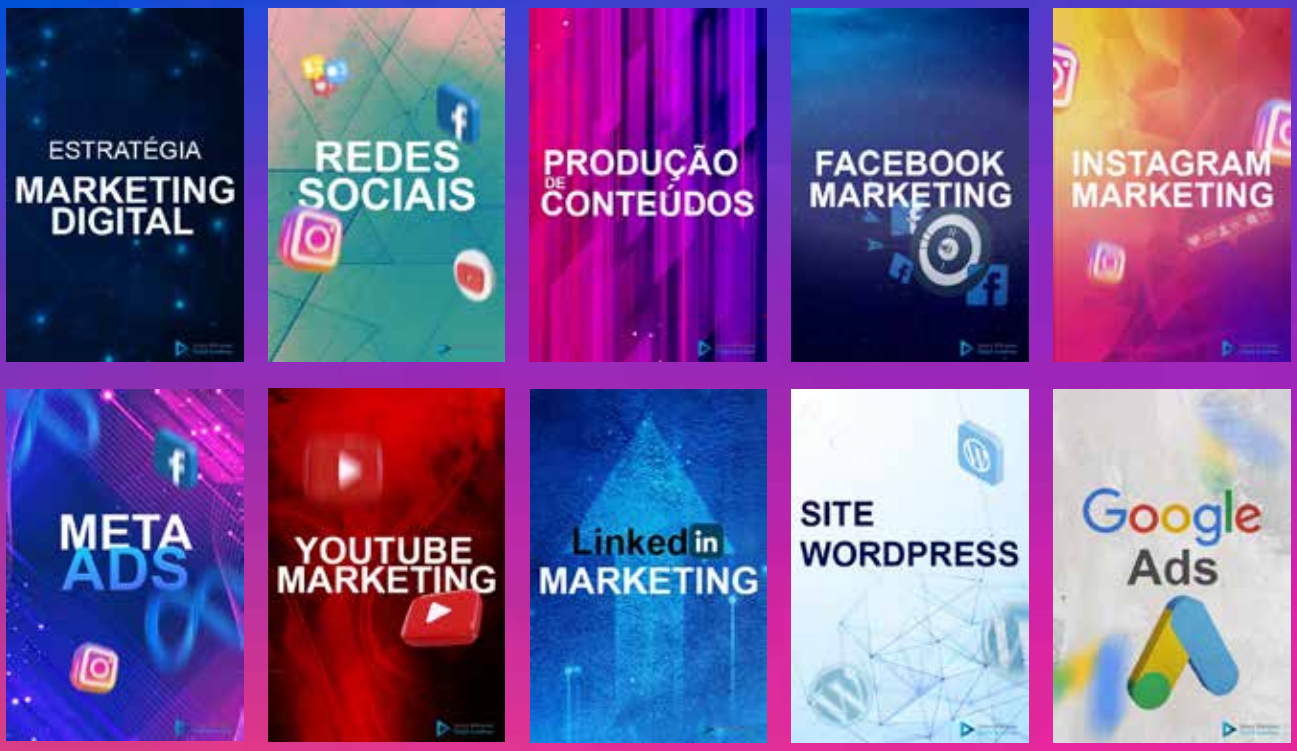
O maior desafio é o ritmo a que as ameaças evoluem. As empresas precisam de formação constante, mas também de abordagens personalizadas, porque cada uma tem a sua cultura. Na MEO apostamos em programas de cyber awareness. Desde 2020, todos os nossos utilizadores são alvo de campanhas simuladas de phishing e têm formação contínua, o que ajuda à adopção de boas práticas de segurança no seu dia-a-dia.

Olhando para os próximos anos, quais são as principais tendências e ameaças que vão marcar a cibersegurança nas telecomunicações, na visão da MEO?

Acreditamos que o ransomware e o phishing vão continuar a ser ameaças muito relevantes. A cloud, a mobilidade e as metodologias ágeis vão trazer novos desafios. Por outro lado, a inteligência artificial terá um papel cada vez mais importante na defesa e na análise preditiva. A nossa estratégia passa por continuar a investir nestas áreas e por reforçar a colaboração com o governo, operadores e sector privado, para que possamos enfrentar este ecossistema de ameaças de forma coordenada e eficaz. ●

Curso 100% online

MARKETING DIGITAL de A a Z



MAIS INFORMAÇÕES:

800 450 360

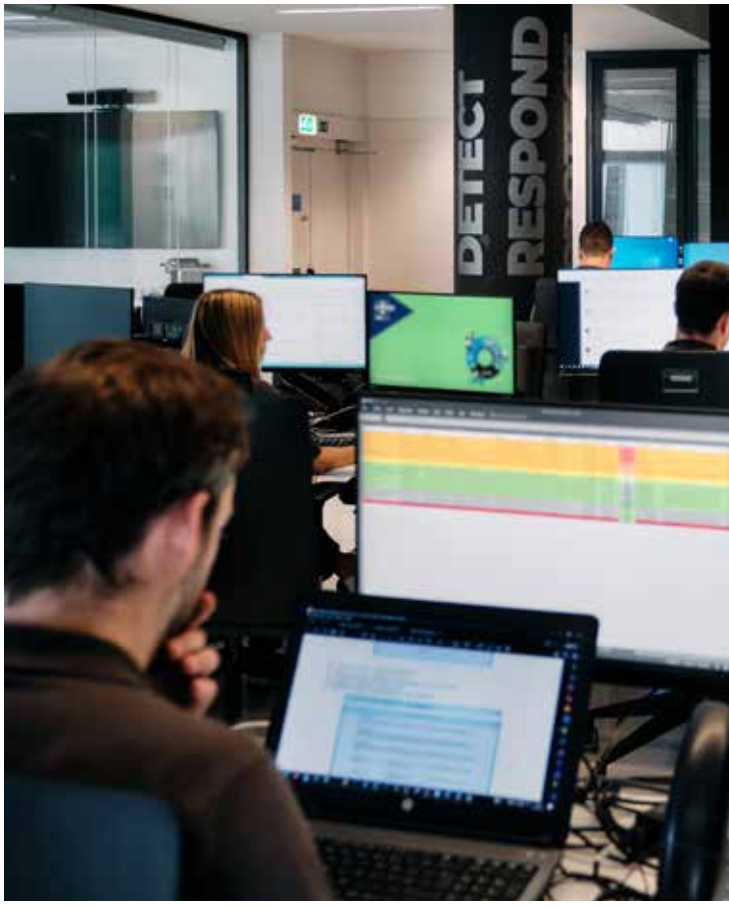
CHAMADA GRÁTIS

WWW.VASCOMARQUES.ACADEMY

DGERT ENTIDADE FORMADORA CERTIFICADA

W2B Web2Business

Vasco Marques Digital Academy



SIBS CYBERWATCH

COMO A SIBS CYBERWATCH TRANSFORMA RISCO EM VANTAGEM COMPETITIVA

INTEGRAR TECNOLOGIA, PESSOAS E PROCESSOS É HOJE O SEGREDO PARA INOVAR COM SEGURANÇA

As empresas estão a inovar mais depressa do que conseguem proteger-se. Entre a adopção de IA, cloud e automação, surgem novas vulnerabilidades todos os dias.

«Há um desfasamento claro entre a velocidade com que as novas tecnologias são adoptadas e a capacidade das equipas de segurança para adaptarem processos e estratégias», explica Fausto Curado, Head of SIBS CyberWatch. «Mais do que um desafio técnico, é uma questão estratégica e humana.»

Com uma oferta pensada para abordar esta emergente realidade, a SIBS CyberWatch disponibiliza soluções de externalização da gestão de eventos e segurança da informação — permitindo às empresas focarem-se no seu core —,sistemas de alarmística, apoio na criação de processos de resposta e contenção de ameaças, testes de penetração e suporte na definição de políticas de segurança alinhadas com a regulação em vigor.

A inteligência artificial é exemplo maior de como uma ferramenta pode ter um efeito dramático no incremento dos riscos para as organizações, mas também pode uma verdadeira aliada estratégica na segurança digital. Na SIBS CyberWatch a visão passa pela utilização da tecnologia para navegar na complexidade e transformar a segurança num motor de eficiência e confiança.

Como explica Fausto Curado, «a adopção destas ferramentas é inevitável, mas deve ser feita com inteligência». É precisamente aqui que entra o apoio da SIBS CyberWatch — ajudando as empresas a modernizar-se sem abrir brechas na sua defesa. A IA é usada para dar contexto e relevância à informação, adaptando-se à realidade de cada sector e negócio. Em vez de se limitar a detetar anomalias, passa a antecipar riscos e a prever comportamentos antes que estes tenham impacto.

A tecnologia da SIBS CyberWatch filtra o ruído e destaca apenas o que realmente importa, libertando as equipas para se concentrarem nas decisões críticas e nos incidentes que exigem intervenção humana. A monitorização contínua garante ainda que nenhuma ameaça passa despercebida, mesmo num cenário em rápida evolução. O resultado é um ecossistema mais resiliente e preparado, onde a inovação e a

segurança coexistem de forma equilibrada — porque a confiança é o verdadeiro ativo digital do futuro.

E se há algo que distingue esta abordagem é o seu foco nas pessoas. «A IA não substitui especialistas — potencia o seu foco e capacidade de resposta», sublinha o responsável.

Pessoas no centro da defesa digital

Numa era em que as ameaças digitais se tornam cada vez mais sofisticadas, a tecnologia por si só não basta. Na SIBS CyberWatch, o investimento vai tanto para tecnologia quanto para as pessoas — porque a resiliência começa nas equipas.

Fausto Curado lembra que a capacitação das equipas é o motor que transforma tecnologia em verdadeira protecção. «Equipas treinadas identificam sinais de ataque antes que causem danos, tal como um radar antecipa uma tempestade», explica. Em vez de reagirem apenas a incidentes, os profissionais desenvolvem uma postura proactiva, antecipando ameaças e reduzindo riscos de impacto.

A IA NÃO SUBSTITUI ESPECIALISTAS POTENCIA O SEU FOCO E CAPACIDADE DE RESPOSTA

O treino em ambientes simulados aumenta a rapidez e precisão da resposta, permitindo que os colaboradores apliquem procedimentos já interiorizados e neutralizem ameaças com eficácia. Além disso, equipas bem preparadas conseguem traduzir riscos técnicos em linguagem clara para a gestão, tornando a cibersegurança uma prioridade estratégica em toda a organização.

A combinação de automação e proactividade não só aumenta a eficiência operacional, reduzindo o tempo de resposta a incidentes, como também garante uma evolução contínua da capacidade de detecção e mitigação de ameaças. Tecnologia como detecção avançada e plataformas de monitorização só atingem o seu potencial quando apoiadas por analistas qualificados, e esses analistas só brilham quando equipados com treino contínuo e processos claros.

SEGURANÇA QUE FALA A LINGUAGEM DA GESTÃO

Um ciberataque pode ter efeitos catastróficos nas organizações. A cibersegurança deve ser promovida internamente pelas lideranças e encarada como uma prioridade executiva. É por isso que priorizar a cibersegurança já não é apenas uma questão de TI — é uma prioridade estratégica que impacta diretamente a gestão e a competitividade. Com modelos reconhecidos como NIST, ISO 27001, NIS2 e DORA, a SIBS CyberWatch ajuda as empresas a alinhar segurança e regulamentação sem duplicar esforços, transformando requisitos técnicos em resultados de negócio claros.

Qualquer processo ou tecnologia é insuficiente sem uma cultura de segurança consolidada», sublinha Fausto Curado. Na prática, isso significa capacitar equipas, automatizar tarefas repetitivas e garantir que cada colaborador atua como um sensor ativo, fortalecendo a defesa da organização.

«Transformamos dados técnicos em decisões estratégicas, permitindo que a segurança se torne um ativo de gestão», reforça Fausto Curado. Ao ligar riscos técnicos ao impacto real no negócio, a SIBS CyberWatch cria eficiência, reduz o ruído de alertas e liberta as equipas para tarefas de maior valor. A solução integra ainda uma cultura de responsabilidade partilhada, tornando a cibersegurança transversal à governança empresarial e central na estratégia de resiliência.

Fausto Curado descreve alguns casos em que esta ligação com a liderança foi crítica. Uma instituição financeira que solicitou apoio na implementação de uma solução de monitorização e resposta a incidentes de segurança. A equipa interna de IT não tinha recursos dedicados à cibersegurança nem visibilidade sobre as ameaças activas. O efeito da intervenção foi significativo, como a redução de

» Fausto Curado, Head of SIBS CyberWatch

60% no tempo médio de deteção e resposta (MTTD/MTTR) e a eliminação de falsos positivos críticos através da correlação de eventos e contextualização via Threat Intelligence.

Fausto Curado descreve ainda outro caso de um cliente, em que a equipa CyberWatch conseguiu reduzir a fraude em 85%, com mais de 5.000 takedowns de campanhas de phishing, perfis falsos e sites fraudulentos. Estes resultados demonstra como a aplicação prática da cibersegurança, com suporte da liderança, pode gerar valor real e mensurável para o negócio, protegendo ativos e reforçando a confiança digital.

SEGURANÇA COM ADN SECTORIAL

Cada sector tem riscos, prioridades e linguagens próprias. Na SIBS CyberWatch, a cibersegurança adapta-se a cada realidade, transformando ameaças em oportunidades de proteção estratégica. As equipas são constituídas por profissionais altamente especializados, com experiência comprovada em ambientes críticos e regulados, como banca, farmacêutica e outros sectores sensíveis.

Fausto Curado reforça que há características e desafios de cada setor, reconhecendo que a natureza dos riscos, o enquadramento regulatório e o impacto no negócio variam entre indústrias. No setor financeiro, por exemplo, a prioridade está na deteção de malware bancário, fraudes e ataques a canais digitais; na saúde, o foco recai sobre a proteção de dados clínicos e a continuidade de sistemas críticos; já na indústria, ganha relevo a segurança operacional e a proteção de infraestruturas conectadas.

A CyberWatch conta com analistas SOC (níveis L1 a L3), engenheiros de segurança, especialistas em Threat Intelligence, analistas de malware e peritos em resposta a incidentes, todos com certificações reconhecidas internacionalmente. Esta experiência permite oferecer soluções personalizadas e alinhadas com as necessidades de cada cliente, antecipando riscos e garantindo conformidade regulatória.

Entre os serviços disponibilizados destacam-se:

- SOC 24x7 — monitorização contínua com SIEM gerido, integrando logs de endpoints, firewalls, proxies e aplicações críticas.
- MDR — detecção e resposta gerida (EDR) em endpoints e servidores, com playbooks automáticos de contenção.
- CTI — enriquecimento de alertas com fontes de inteligência de ameaças e relatórios de tendências adaptados ao sector financeiro.
- Pentesting — testes de intrusão trimestrais para avaliar a eficácia das defesas e validar correções.
- GRC — definição de políticas de segurança, matriz de riscos e apoio à conformidade regulatória.

Ao oferecer soluções e abordagens ajustados a cada realidade, a SIBS CyberWatch permite que a segurança se torne verdadeiramente operacional e estratégica, sustentando a resiliência e a competitividade de cada organização.

O FUTURO? MAIS E MAIS RÁPIDA INOVAÇÃO

O futuro da cibersegurança obriga a mais e melhores respostas de resiliência, combinando tecnologia avançada com estratégias de negócio integradas, incluindo IA generativa, Security-by-Design, arquitetura Zero Trust e monitorização da cadeia de fornecimento digital. Como destaca Fausto Curado, «as organizações mais bem preparadas serão aquelas que compreendem a cibersegurança como um 'sistema imunitário vivo', capaz de se adaptar e prosperar mesmo em ambientes incertos».

É por isso que a cibersegurança deixou de ser apenas uma função técnica para se afirmar como elemento estratégico, indispensável à resiliência, competitividade e inovação das organizações. A integração completa de tecnologia, processos, formação contínua e cultura organizacional transforma cada ameaça numa oportunidade de reforçar a segurança e criar valor sustentável. ●

auto. monitor

A abordagem 360º ao mundo automóvel

MERCADO

TECNOLOGIA

RENTING & FROTAS

NOVIDADES

MARKETING & PUBLICIDADE

PRODUTOS & SERVIÇOS

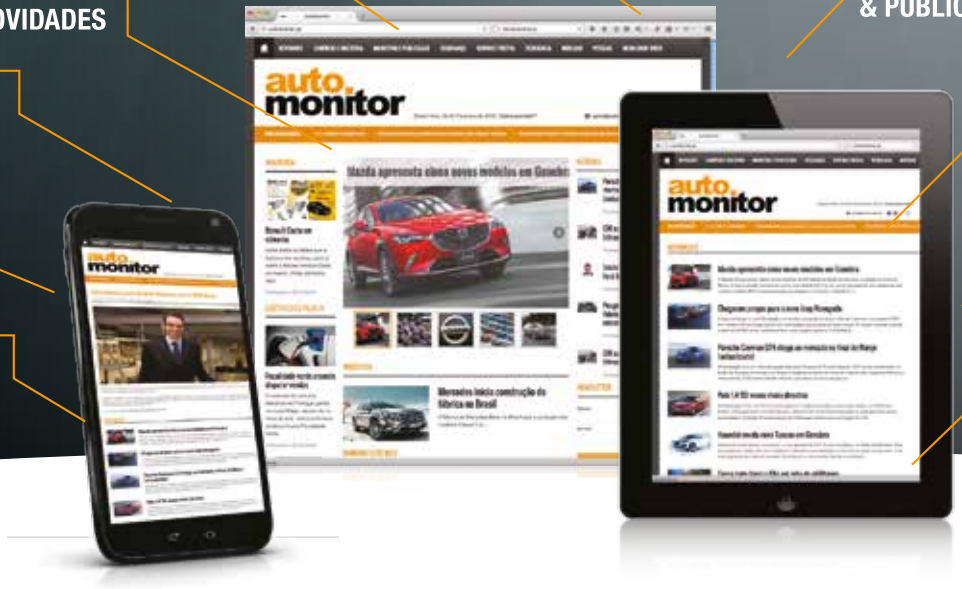
SEGURANÇA

PESSOAS

VIAS DE CIRCULAÇÃO

COMÉRCIO E INDÚSTRIA

MOBILIDADE VERDE



automonitor.pt

ZURICH

RISCOS DIGITAIS E IA: O FUTURO DA PROTECÇÃO

O AUMENTO DA DIGITALIZAÇÃO E DA COMPLEXIDADE TECNOLÓGICA TEM COLOCADO AS EMPRESAS PORTUGUESAS PERANTE NOVOS DESAFIOS EM MATÉRIA DE CIBERSEGURANÇA

Riscos como ataques de ransomware, phishing, comprometimento das cadeias de fornecimento e ameaças geopolíticas exigem respostas estratégicas e adaptáveis. No mês dedicado à cibersegurança, a Executive Digest conversou com Pedro Pinto, head of Information Security na Zurich Portugal, sobre as tendências emergentes, o impacto da inteligência artificial (IA), a gestão do risco humano e o papel das seguradoras na protecção das organizações.

Quais os principais riscos cibernéticos que as empresas portuguesas enfrentam e qual o papel de uma seguradora neste contexto?

Embora os riscos cibernéticos sejam transversais e não se limitem a fronteiras nacionais, a nossa experiência operacional e a monitorização contínua do panorama de ameaças permitem identificar quatro riscos principais para a segurança digital das empresas em Portugal: ransomware, comprometimento das cadeias de fornecimento, phishing e engenharia social e a instabilidade geopolítica.

Os ataques de ransomware continuam a ser uma das ameaças mais significativas, pela sofisticação crescente e capacidade de adaptação, que tornam a detecção precoce e a resposta eficaz cada vez mais

difíceis. Também o comprometimento das cadeias de fornecimento é uma tendência preocupante, já que ataques a prestadores de serviços tecnológicos têm afectado indirectamente grandes organizações, exigindo maior rigor na avaliação e monitorização de terceiros.

As campanhas de phishing e engenharia social, potenciadas pela IA generativa, atingiram níveis sem precedentes. Esta evolução obriga a reforçar mecanismos de detecção e autenticação, bem como a apostar na formação contínua dos colaboradores, que são a primeira linha de defesa.

A instabilidade geopolítica global é outro factor que tem vindo a influenciar directamente o panorama da cibersegurança. Para além do aumento de ataques motivados por interesses políticos, começamos a observar restrições à utilização de determinadas tecnologias em função da sua origem geográfica. Este factor poderá, num futuro próximo, obrigar as organizações a rever as suas estratégias de aquisição e dependência tecnológica, com impacto directo na continuidade operacional.

Num contexto cada vez mais digital e exposto a riscos, as seguradoras assumem um papel estratégico na protecção das organizações, contribuindo para a prevenção, mitigação e recuperação face a incidentes de segurança digital. Este contributo concretiza-se na prevenção – com avaliações de risco, conteúdos formativos e apoio ao cumprimento de obrigações legais como o Regulamento Geral sobre a Protecção de Dados (RGPD) – e na protecção e resposta, através de produtos específicos que cobrem riscos cibernéticos e suporte especializado na recuperação, essenciais para minimizar impactos financeiros, operacionais e reputacionais que podem resultar de um ataque.

«A NOSSA ABORDAGEM É PROACTIVA, COM EQUIPAS MULTIDISCIPLINARES QUE MONITORIZAM DIRECTIVAS COMO O NIS2 OU O DORA, AVALIANDO O IMPACTO E ASSEGURANDO RESPOSTAS ÁGEIS»

Em Portugal, a Zurich aposta na prevenção e capacitação, automatizando processos para reduzir riscos, promovendo formação em cibersegurança e acompanhando de perto as regulamentações europeias e nacionais, ajudando clientes e parceiros a adaptar-se e a cumprir requisitos legais. Num cenário de crescente complexidade digital, as seguradoras posicionam-se como parceiros estratégicos das empresas portuguesas, contribuindo para um ecossistema empresarial mais seguro, resiliente e preparado para enfrentar os desafios do ciberespaço.

Como é que a Zurich acompanha as rápidas mudanças na regulação europeia, como o NIS2 ou o DORA?

Num contexto empresarial dinâmico e regulado, a adaptação às exigências legais tornou-se um factor crítico de sucesso. Na Zurich, vemos a conformidade não apenas como obrigação, mas como um compromisso estratégico com a confiança, resiliência e segurança dos clientes e parceiros.

Encaramos a evolução regulatória como oportunidade para reforçar processos, consolidar práticas de excelência e antecipar riscos emergentes. A nossa abordagem é proactiva e colaborativa, envolvendo equipas multidisciplinares que monitorizam continuamente novas directivas e regulamentações, avaliando o seu impacto e assegurando uma resposta ágil e eficaz.

Entre as iniciativas que temos vindo a desenvolver, destaco o reforço da resiliência operacional, com foco na continuidade de negócio e na capacidade de resposta a incidentes, a melhoria dos processos de gestão de activos tecnológicos, garantindo maior visibilidade e controlo sobre o nosso inventário de TI e, por fim, a implementação de controlos avançados de conformidade, que nos permitem avaliar com maior precisão o risco residual e alinhar os nossos sistemas com os requisitos legais mais exigentes.

Complementamos estas acções com workshops temáticos dirigidos aos nossos colaboradores e parceiros de negócio, com vista a apoiá-los na compreensão e implementação das melhores práticas exigidas pela legislação para, assim, estarem preparados para os desafios futuros.

Na Zurich, consideramos que a segurança e a conformidade são pilares indissociáveis da confiança. É com este princípio que desenhamos as nossas soluções e fortalecemos a nossa posição como parceiro de referência no sector segurador.

A inteligência artificial já é usada tanto para atacar como para defender. Como vê a Zurich o impacto da IA no futuro da cibersegurança?

A inteligência artificial (IA) está a transformar profundamente o panorama da cibersegurança e na Zurich acompanhamos esta evolução com atenção e responsabilidade. Reconhecemos que

a IA representa uma mudança de paradigma – não apenas pela sofisticação das ferramentas que coloca ao nosso dispor, mas também pelos novos riscos que introduz.

Por um lado, a IA permite-nos reforçar significativamente as nossas capacidades de protecção: conseguimos identificar ameaças com maior rapidez e precisão, avaliar o seu impacto real, automatizar respostas e até antecipar comportamentos maliciosos antes que se concretizem. Estas capacidades são hoje integradas em sistemas como o nosso SIEM (Security Information and Event Management), que recorre à IA para analisar grandes volumes de dados e gerar respostas automáticas em tempo real.

Estamos também a aplicar a IA no processo de gestão de vulnerabilidades, atribuindo prioridades de remediação com base numa análise contextual e inteligente do risco. Esta abordagem permite-nos optimizar recursos e actuar com maior eficácia na proteção dos nossos activos.

Por outro lado, não ignoramos que estas tecnologias estão a ser exploradas por agentes maliciosos, que as utilizam para desenvolver ataques mais sofisticados – e com maior potencial de disrupção. Na nossa visão, a IA representa uma oportunidade única para criar uma protecção mais inteligente e uma resposta mais rápida, mas exige também uma abordagem e utilização ética e responsável. Por isso, na Zurich, assumimos o compromisso de colocar a tecnologia ao serviço das pessoas e das empresas, contribuindo para um futuro digital mais seguro, resiliente e confiável.

As falhas humanas continuam a ser um dos maiores riscos na cibersegurança. De que forma se pode contrariar este risco e transformá-lo numa oportunidade?

No universo da cibersegurança, as falhas humanas continuam a ser um dos riscos mais relevantes. Contudo, na Zurich, optamos por encarar este desafio como uma oportunidade para fortalecer a nossa cultura organizacional e reforçar a nossa proteção digital.

Recentemente, observámos casos concretos de organizações globais que sofreram disrupções significativas nas suas operações de suporte, na sequência de ataques de vishing. Estes episódios sublinham a importância de capacitar os colaboradores para reconhecer e reagir a ameaças cada vez mais sofisticadas.

Por isso, investimos de forma contínua em acções de formação e sensibilização, com o objectivo de promover práticas seguras e manter os nossos colaboradores actualizados face às ameaças emergentes. Esta aposta representa um pilar essencial da nossa estratégia de cibersegurança, permitindo-nos transformar o risco em vantagem competitiva.

Ao envolvermos os nossos colaboradores como agentes activos na protecção da organização, fomentamos uma cultura de segurança partilhada, onde a responsabilidade é transversal e integrada no quotidiano da empresa.

Complementarmente, recorremos à tecnologia como aliada estratégica. Soluções que simplificam processos e automatizam tarefas contribuem para reduzir a probabilidade de falha humana. Sistemas inteligentes permitem identificar comportamentos anómalos e emitir alertas em tempo útil, possibilitando uma resposta rápida e eficaz.

Em suma, na Zurich, acreditamos que as falhas humanas – quando abordadas com responsabilidade e visão – podem ser um impulsionador de evolução.

Em caso de ataque, quais as fases de apoio que a Zurich garante, desde a detecção até à recuperação?

Na Zurich, reconhecemos que a capacidade de resposta a incidentes de segurança é um dos pilares fundamentais da resiliência organizacional. Por isso, contamos com equipas especializadas, preparadas para actuar em todas as fases do ciclo de resposta, garantindo uma intervenção rápida, eficaz e orientada para minimizar impactos e acelerar a recuperação do negócio.

A nossa abordagem estrutura-se em cinco fases principais: detecção e notificação, resposta ime-

» Pedro Pinto, head of Information Security na Zurich Portugal

diata, investigação e análise, contenção e remediação, recuperação e aprendizagem. Graças a procedimentos bem definidos conseguimos actuar com agilidade e assertividade em cada uma destas fases, reforçando a confiança dos nossos clientes e parceiros.

Os testes que realizamos com frequência são essenciais para aferir o nosso nível de prontidão. Permitem-nos identificar oportunidades de melhoria, corrigir desvios e garantir que, em caso de incidente, a resposta será eficaz e alinhada com as melhores práticas do sector.

Encaramos a resposta a incidentes não apenas como uma reacção, mas como uma componente estratégica da nossa missão de proteger pessoas, empresas e activos num mundo digital em constante transformação.

Que tendências em cibersegurança considera mais relevantes para os próximos anos e de que forma a Zurich se está a preparar para responder a esse futuro?

A cibersegurança está a atravessar uma fase de transformação acelerada, impulsionada por avanços tecnológicos e pela crescente complexidade das ameaças. Na Zurich, identificamos algumas das tendências mais relevantes que irão moldar o sector nos próximos anos e que exigem uma resposta estratégica por parte das organizações.

Destacamos o crescimento exponencial da IA, que tanto potencia novas capacidades defensivas como é explorada por agentes maliciosos para desenvolver ataques mais sofisticados. O aumento de ataques direccionados a infraestruturas críticas – como os de DDoS (Distributed Denial of Service) – e a indivíduos – através de técnicas avançadas de phishing e vishing – são também preocupações centrais. A sofisticação crescente do ransomware e a necessidade urgente de proteger ambientes híbridos e remotos completam este quadro de risco.

Simultaneamente, temas como a privacidade dos dados, o cumprimento das regulamentações e a resiliência operacional ganham uma importância estratégica crescente nos dias de hoje. Estes factores exigem uma abordagem integrada, multidisciplinar e proactiva da gestão do risco para proteger tanto empresas como cidadãos.

Na Zurich, estamos atentos a este cenário em constante evolução. Investimos em inovação tecnológica, estabelecemos parcerias estratégicas e promovemos o desenvolvimento contínuo de competências técnicas dos nossos colaboradores, para que estejam capacitados para apoiar os nossos clientes e parceiros na gestão eficaz destes riscos.

Outra estratégia que adoptámos é o reforço das nossas soluções de cibersegurança com ferramentas avançadas de monitorização, resposta a incidentes e análise preditiva, combinando tecnologia de ponta com o conhecimento especializado das nossas equipas.

«DO LADO DA DEFESA, A IA REFORÇA AS NOSSAS CAPACIDADES: PERMITE IDENTIFICAR AMEAÇAS COM MAIOR RAPIDEZ E PRECISÃO, AUTOMATIZAR RESPOSTAS E ANTECIPAR COMPORTAMENTOS MALICIOSOS»

O nosso compromisso é estar ao lado dos nossos clientes e ajudá-los a aumentar a sua resiliência face aos riscos cibernéticos, antecipando tendências e oferecendo protecção ajustada à realidade de cada negócio.

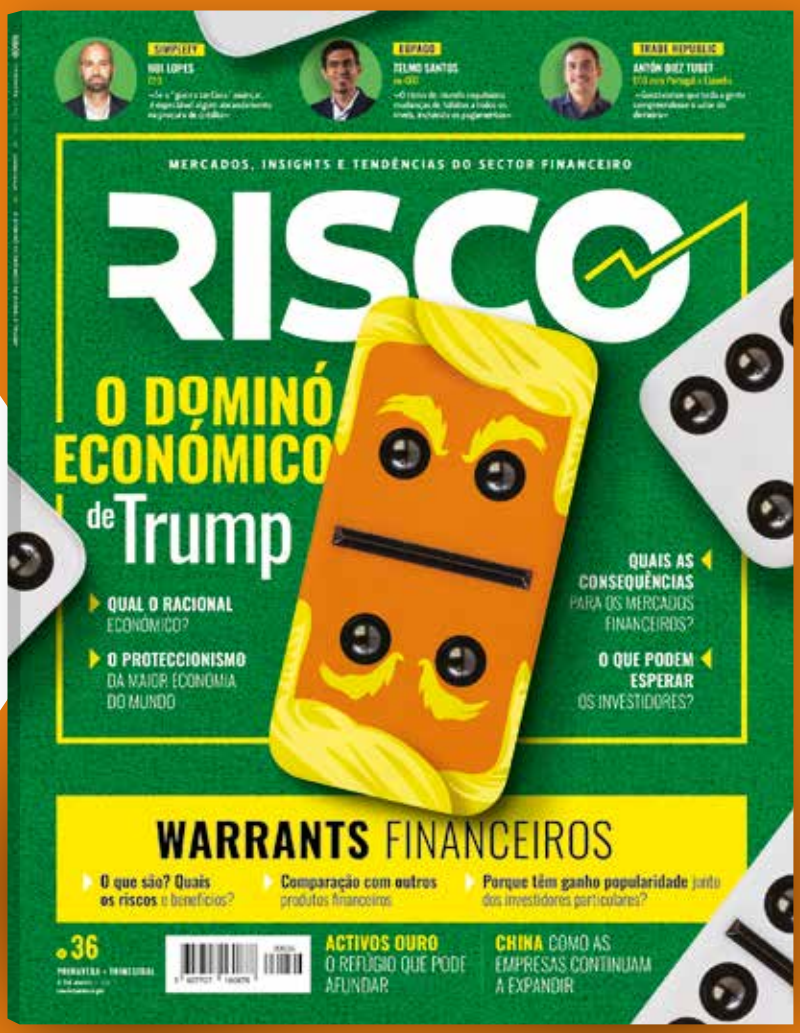
Neste mês dedicado à cibersegurança, de que forma a Zurich assinala e promove esta iniciativa?

Ao longo de todo o ano disponibilizamos conteúdos digitais sobre cibersegurança aos nossos colaboradores. Também há nove anos que, neste mês de Outubro, promovemos o "Mês da Sensibilização para a Cibersegurança" na Zurich Portugal e globalmente para mais de 200 países e territórios onde a Zurich está presente. Temos procurado fomentar um conjunto diversificado de actividades – desde conteúdos educativos, workshops e jogos interactivos – com o objectivo de reforçar o envolvimento e a consciencialização interna sobre estes temas.

A implementação desta iniciativa assume uma importância extrema para nós – representa uma oportunidade adicional para promovermos boas práticas de segurança e reforça a importância de protegermos os nossos clientes e os seus dados, compromisso ancorado numa cultura de cibersegurança sólida e robusta. ●

1 ANO
ASSINATURA
4 EDIÇÕES*
€10,40

2 ANOS
ASSINATURA
8 EDIÇÕES*
€18,50



NÃO ARRISQUE, APROVEITE E ASSINE.

RECEBA A SUA ASSINATURA EM CASA OU NO ESCRITÓRIO!

Para mais informações ligue **210 123 400** ou email **assinaturas@multipublicacoes.pt**
Assine já em: **https://assinaturas.multipublicacoes.pt/**

VALORES VÁLIDOS PARA **CONTINENTE E ILHAS**