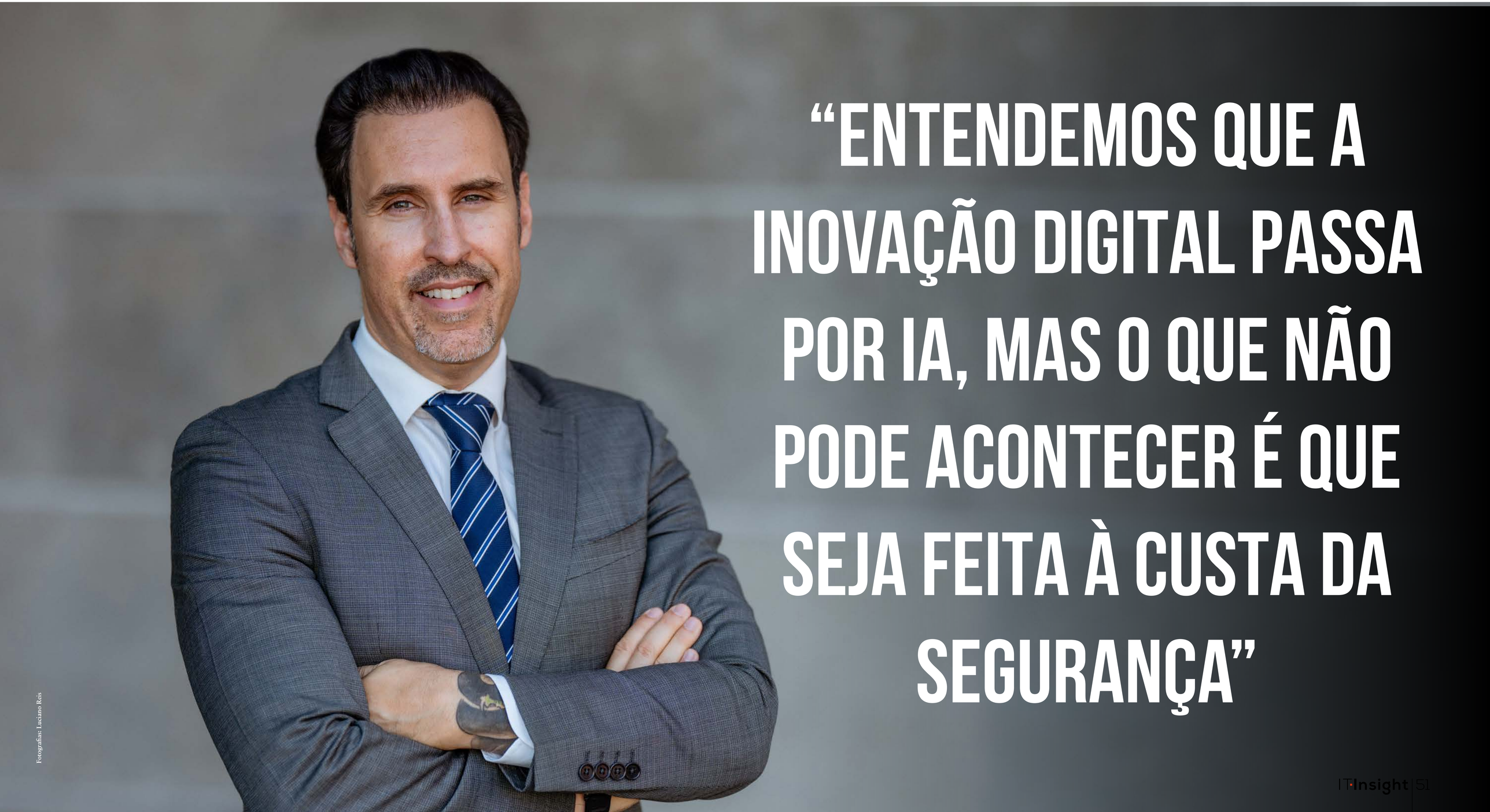
BRUNO CASTRO, FOUNDER & CEO DA VISIONWARE



"ENTENDEMOS QUE A INOVAÇÃO DIGITAL PASSA POR IA, MAS O QUE NÃO PODE ACONTECER É QUE SEJA FEITA À CUSTA DA SEGURANÇA"

Fotografias: Luciano Reis

Bruno Castro, Founder & CEO da VisionWare, aborda em entrevista o estado atual da cibersegurança e da inteligência artificial como uma ameaça, desde o "turning point" até às ameaças atuais à forma como as organizações abordam os seus processos.

RUI DAMIÃO

A VISIONWARE ACABOU DE COMPLETAR 20 ANOS E ESTÁ NUMA FASE DE EXPANSÃO INTERNACIONAL, ESPECIALMENTE EM CABO VERDE. QUAL É A LÓGICA ESTRATÉGICA POR TRÁS DESTA APOSTA QUANDO MUITAS EMPRESAS PORTUGUESAS DE TECNOLOGIA SE FOCAM NO MERCADO EUROPEU?

A VisionWare faz 20 anos, mas sempre tivemos o mercado internacional como horizonte. A VisionWare começou em 2005 e, de forma quase instantânea, criámos logo *networking* para saltar para o mercado internacional porque sabíamos que, há 20 anos, o mercado da cibersegurança não era exequível só no mercado nacional.

Cabo Verde foi uma das geografias que abordámos e trabalhámos. Nos primeiros cinco, dez anos, fizemos muitos processos de *fly in, fly out*, em consórcios e parcerias, muito ligado a consórcios internacionais para a Comissão Europeia, muitas oportunidades de negócio via Ministério da Defesa, que chegámos a ter, depois, como acionista.

Tivemos um projeto através do Banco Mundial de Investimento para auditar e montar o modelo de segurança do Banco Central de Cabo Verde, financiado pelo BMI, via Washington, e aparecemos no radar. Fomos convidados para uma *shortlist* e concorremos a dezenas de concursos internacionais.

Depois de estarmos a trabalhar em Cabo Verde percebemos que o setor financeiro, as telco, o governo e até o tecido empresarial com financiamento ou ligação portuguesa estava muito forte e enraizada em Cabo Verde e, imediatamente, há um *gap* no mercado que achámos que podíamos complementar, que era a área da cibersegurança e do *compliance*.

Diria que passou a ser estratégico porque criámos uma operação física lá

através de um convite do próprio governo na criação dos dois polos – o Techpark que há em São Vicente e em Praia – em que o governo nos desafia, ao fim de sete anos de presença em Cabo Verde, com grande parte do mercado e experiência muito próxima. Passou a fazer parte da nossa estratégia de crescimento, com recrutamento local e formação em Portugal. Hoje, temos uma operação de 40 pessoas em Cabo Verde, distribuídas por dois polos, que são fundamentais para nós. Aliás, quando foi o apagão, a nossa operação de SOC trabalhou 100% através de Cabo Verde.

NO PASSADO, O BRUNO DEFINIU O ATAQUE À VODAFONE, EM 2022, COMO O GRANDE *"TURNING POINT"* DA CIBERSEGURANÇA EM PORTUGAL. EM 2025, ONDE É QUE ESTÁ PORTUGAL EM TERMOS DE MATURIDADE CIBERNÉTICA? MELHORÁMOS, FICÁMOS APENAS MAIS CONSCIENTES OU ESTAMOS IGUAIS?

Nós que trabalhamos na área da cibersegurança temos a mania de que somos muito inteligentes e muito espertos, sabemos tudo e temos um ego grande. Diria que a primeira dose de humildade que levei foi o ataque à Vodafone. Se me perguntassem horas antes se era possível uma operadora como a Vodafone, com a maturidade que tem, ter um apagão daqueles em que quatro milhões de pessoas estão em *off* durante horas, diria que é impossível. Começámos a repensar que, aquilo que achávamos que era um nível de maturidade muito sólido, se calhar não era assim tão sólido ou tão resiliente. Começámos a ponderar muito aquilo que tínhamos como critérios de estabilidade e resiliência e solidez na cibersegurança.

Depois começaram a existir ataques sucessivos, altamente disruptivos, em termos de roubo de informação e exposição ou mesmo em termos de disrupção violenta em que caíram serviços. Todas elas foram mais doses de humildade.

Diria que hoje, nós que trabalhamos no setor da cibersegurança, mesmo com 20, 25 anos de experiência no terreno, olhamos para o mundo da cibersegurança e para a gestão de risco, modelos de resiliência, de segurança, de maturidade, com olhos muito mais desconfiados. Não temos tantas certezas como tínhamos antes. Acho que esse paradigma mudou para quem fornece

serviços de cibersegurança. Deixou de haver tantas verdades absolutas, em que se investir 'x', vai ter '*y*' nível de robustez.

Passámos a estar muito mais atentos, através da nossa unidade de *intelligence*, não só à atividade de grupos cibercriminosos conhecidos, mas também ao que eles sabem fazer. Não só àquilo que se passa nos fóruns ou nos meios académicos, mas perceber de forma infiltrada o que é que grupos criminosos andam a fazer em termos de novos conhecimentos, novas *skills*, novos mecanismos, novos consórcios que montam para perceber o que é que vêm a seguir.

Passado este tempo todo, o mercado hoje, em Portugal, está mais sólido, maduro e robusto? A minha resposta instantânea é sim. Há 25 anos, quando falávamos de cibersegurança era impossível falar sobre isto de uma forma clara para um gestor de topo. Não percebia o investimento, porque era um custo, essencialmente. Estávamos a falar sobre algo que poderia vir a acontecer um dia, talvez. Era tudo muito esotérico, muito difícil de explicar o retorno de investimento.

Hoje já não existe essa conversa com um gestor de topo moderno; ele sabe perfeitamente que tem de ter o seu negócio ou atividade no ciberespaço e sabe perfeitamente os riscos que isso acarreta para o seu negócio e para a sua marca – seja ela da empresa ou pessoal.

Se a pergunta é sobre o nível de robustez das instituições hoje em Portugal, se está mais acima do que era há cinco ou dez anos, sim, claramente. Não é só pelo nível de investimento que fazem em termos de aquisição de infraestrutura ou tecnologia; é muito mais pelos modelos de segurança que montam internamente, o auditar-se a si próprio já não é um tema que melindre. Avaliar o nível de *awareness*, a formação dos colaboradores já é natural e

não há barreiras para isso. Criar restrições à liberdade digital também já não é tema; faz parte. Diria que esses modelos de novas e boas práticas são facilmente distribuídas e são muito premiáveis à gestão de topo e até ao *middle management*.

Acredito que existe uma desproporção grande ainda no nível de maturidade das empresas, daquilo que têm de guardar e proteger dos ativos digitais que estão a pôr no ciberespaço, face à ameaça que existe. Há uma desproporção, mas estamos melhores.

OS ÚLTIMOS DOIS ANOS TÊM SIDO DE GRANDE REVOLUÇÃO REGULAMENTAR, COM A ENTRADA EM VIGOR DA NIS2 E DA DORA. AS EMPRESAS PORTUGUESAS ESTÃO PREPARADAS PARA ESTES NOVOS REQUISITOS OU VAMOS ASSISTIR A UMA AVALANCHE DE INCUMPRIMENTOS?

Por um lado, vejo que estes normativos e obrigações – e já vem desde o tempo do RGPD – vêm acrescentar valor. Não sou daqueles que diz que 'há mais uma obrigação e mais um conjunto de normativos, de leis e de obrigações' e temos de cumprir as *checklists*. Vejo isso como uma necessidade para criar um ecossistema coerente e uniforme entre todos.

Em alguns setores de indústria, temos de cumprir requisitos para estar naquele setor, se não somos expulsos daquele ecossistema. Não é nada de novo. O que me parece é que estas novas regulações – o DORA, a NIS2, o AI Act, RGPD – vêm tornar tangíveis alguns critérios de segurança mínimos que temos de ter para viver no ciberespaço de forma coerente em que não estou a ameaçar o meu colega do lado. Não vejo isso como um problema.

> "A NIS2 PARECE-ME QUE SERÁ O TEMA DA MODA. A ISO 27001 CONTINUA A SER A BASE E CONTINUAMOS A USAR ISSO COMO BASE DE GOVERNAÇÃO, E EXTRAÍMOS DAÍ A ESTRUTURA NECESSÁRIA"

A abordagem que está a ser colocada em cima da mesa mais uma vez – aconteceu com o RGPD e irá acontecer com o NIS2 também – é um alarmismo generalizado porque se não cumprir uma determinada lei vou ter coimas e vou ser perseguido. Acho que esse conceito está mal contado e deve ser invertido, deve ser *bottom-up*, ou seja, monto o meu modelo de segurança na minha organização, esteja em que setor estiver, adequado à minha atividade e daí extraio tudo o que são critérios para responder à NIS2, ao RGPD, ao DORA, ao que for.

UMA PEQUENA EMPRESA QUE EVENTUALMENTE NÃO TENHA DE CUMPRIR COM A NIS2 PODE UTILIZAR A REGULAÇÃO QUE VAI SER TRANSPOSTA PARA A LEI NACIONAL COMO UMA ESPÉCIE DE *FRAMEWORK* PARA AUMENTAR A SUA RESILIÊNCIA?

A pergunta é bastante interessante porque é-nos colocada várias vezes. Temos clientes que não estão abrangidos pela NIS2 e perguntam se a devem seguir. A minha reposta tipicamente é: 'bem, primeiro vamos montar um modelo de segurança, de governação do vosso setor e eventualmente vamos alinhar com a NIS2'. Isto porque a probabilidade de os parceiros dessa empresa terem de cumprir a NIS2, e de obrigarem os seus próprios parceiros a apresentar critérios e evidências de que também cumprem a NIS2 para estarem a falar a mesma linguagem, é alta.

Já o fazemos há muitos anos, mesmo quando o tema era ISO 27001, já o fazíamos e alinhávamos a empresa. Há uma necessidade de ser certificado, mas, se tiverem modelos de governação '*à la*' ISO 27001, e se estiver bem sólida, em qualquer parceiro, cliente ou fornecedor do meu ecossistema a

quem tenha de prestar contas sobre a minha maturidade para comunicar com ele no futuro, posso mostrar um modelo de defesa que é tangível, reconhecido e uma referência.

A NIS2 parece-me que será o tema da moda. A ISO 27001 continua a ser a base e continuamos a usar isso como base de governação, e extraímos daí a estrutura necessária de critérios para responder à NIS2, acrescentamos outros controlos. Diria que uma PME, se nós formos o CISO, vamos claramente garantir que o modelo de governação, em primeira instância, está adequado ao negócio e iremos fazer o caminho para ser *compliant* com NIS 2.

NO ÚLTIMO ANO, A VISIONWARE PUBLICOU O RELATÓRIO "A ANATOMIA DE UM DEEPFAKE". NAS PALAVRAS DO BRUNO, ESTAS TECNOLOGIAS SÃO "MAIS CONVINCENTES E DIFÍCEIS DE DETETAR". QUE TIPO DE ATAQUES ESTÃO A VER NO TERRENO E COMO É QUE AS EMPRESAS PORTUGUESAS SE PODEM PREPARAR PARA ESTA REALIDADE?

A questão dos *deepfakes* vai ser um dos grandes desafios na área do cibercrime. Os *deepfakes* de voz, associados a esquemas 'olá mãe, olá pai' já com voz envolvida, vai ser um tema para os próximos anos muito mais do que é o phishing.

Com o deepfake com voz – e no futuro com voz e imagem –passamos a ter de desconfiar daquilo que ouvimos e vemos. Vai ser ultra disruptivo nos nossos mecanismos de risco. Ter de explicar a um filho que aquilo que ouve e vê tem de ser desconfiado, ou uma pessoa mais idosa, ou até mesmo uma pessoa formada, vai ser difícil explicar que, quando ouvir a voz de alguém, que não é aquela pessoa.

Ataques feitos com deepfake são, tipicamente, ataques personalizados. O esforço envolvido de um grupo criminoso é elevado porque têm de fazer um deepfake de alguém e têm de criar uma estrutura, um contexto de fraude por trás. Isso envolve esforço, tempo e dinheiro. Do ponto de vista financeiro ou económico, tem de haver retorno para o grupo criminoso.

Como é que as pessoas e as empresas se podem proteger? Vou dizer um cliché, mas é *awareness*, informação, explicar o que é um deepfake e como é fácil fazer isso. Como é que, em termos práticos, um CISO implementa regras para combater ações de fraude baseadas em deepfake? Com *compliance*, é com regras e procedimentos.

Houve um caso de um CFO, que foi estudado, e perceberam que estava de férias através das redes sociais da sua família e é feito um deepfake a dizer 'estou de férias, como sabe estamos a fazer um processo de *due diligence* à empresa '*z*'. Não consigo falar aqui através da operadora nacional, comprei um cartão pré-pago na Tailândia e este é o meu número a partir de agora.

> “HÁ UMA TENDÊNCIA PARA QUE AS SOLUÇÕES QUE VÊM COM IA TENHAM ALGUMAS REGALIAS, NOMEADAMENTE PASSAR AO LADO DO CHAPÉU DA SEGURANÇA”

Aquela ordem que tínhamos pensado em fazer é para fazer, dois milhões de euros, vamos avançar com a compra’.

Mandaram esse áudio direto. Todo o contexto fazia sentido. Havia uma história de origem, ele estava de férias, a voz era dele e a operação fazia sentido. Foi executada quase até ao fim. Quando é que foi interrompida: a pessoa de *compliance*, quando foi para fazer a operação de transferência bancária, disse que há um processo interno que diz que operações acima de sete dígitos têm de ser aprovadas presencialmente pelo CFO.

TAMBÉM TEM ALERTADO QUE “O MALWARE GERADO POR IA É SIGNIFICATIVAMENTE MAIS PERIGOSO”. AO MESMO TEMPO, A IA É FUNDAMENTAL PARA A DEFESA DAS ORGANIZAÇÕES. COMO É QUE SE EQUILIBRA ESTA EQUAÇÃO? A CORRIDA ARMAMENTISTA CIBERNÉTICA ESTÁ A SER GANHA POR QUEM ATACA OU POR QUEM DEFENDE?

Entendemos que a inovação digital vai passar pela inteligência artificial. O que não pode acontecer é que seja feita à custa da segurança. O que temos visto é que há uma corrida desenfreada à procura da solução milagrosa para o negócio através de IA e há uma sensação de que, se não utilizo IA, morro dentro de dois dias. Este é o *mindset* generalizado.

Há uma tendência para que as soluções que vêm com IA tenham algumas regalias, nomeadamente passar ao lado do chapéu da segurança. O nosso esforço nesta fase inicial é ‘obrigar’ – entre aspas – a gestão de topo e dizer ‘isto é uma ação muito importante para vocês, têm uma corrida contra o tempo para estarem otimizados através de ações de IA, estamos solidários convosco em relação a isso, mas é obrigatório que as ações de IA passem pelo modelo de governação de segurança como se fosse uma ação qualquer digital’. Este é o desafio número um.

Para quem trabalha no mundo da segurança há este dilema: quem ataca utiliza IA; quem defende utiliza IA. Como é que está aqui este binómio? Ambos utilizam IA há muitos anos. Quando faço análises comportamentais debaixo de um serviço de *security operation center*, estou a analisar o comportamento da pessoa. Estou a usar IA. Quando processo milhões de eventos por minuto, não é exequível ao olho humano e utilizo a inteligência

artificial para processar todo aquele volume gigantesco de informação e só passa para cima o que é exequível ser visto pelo olho humano.

Do lado do cibercrime também é utilizado há muitos anos. O que estamos a ver agora e que é relevante são duas coisas. Primeiro, os ataques que são feitos de forma personalizada, aquilo a que chamamos de *spear phishing*, tem um investimento de tempo e dinheiro para enganar. Vou estudá-lo, perceber quem é a rede de contactos dele, quem é a família, os amigos, os hobbies, o clube, onde é que utiliza os bancos, onde é que faz compras online, para onde é que viaja e faço um perfil via OSINT. Depois, vou criar conteúdos para tentar enganá-lo e fazer *phishing* sobre ele para fazer um ataque, seja ele qual for. Isto custa tempo e dinheiro para o grupo cibercriminoso.

Com a IA posso dizer que quero atacar uma determinada empresa e peço para identificar quatro perfis do C-Level do IT e, depois de os identificar, para criar perfis para cada um deles; familiares, profissionais, redes sociais, tudo. E depois criar conteúdo para cada um deles, baseado nesse perfil. Ainda pedimos para enviar o conteúdo malicioso para cada um deles de quatro em quatro horas ou de dois em dois dias. Quando o alvo cair, avisa o grupo cibercriminoso. Entretanto, fazemos isso para a empresa A, a B, a C e a D. O cibercriminoso vai ver a bola enquanto a IA trabalha. Transformou um ataque que era altamente personalizado, *high skills*, *time consuming* e que obrigava a muito investimento, num ataque que é massivo e robotizado e com uma alta probabilidade de sucesso.

QUE CONSELHOS DEIXA PARA OS LÍDERES DE CIBERSEGURANÇA E DE TRANSFORMAÇÃO DIGITAL DAS ORGANIZAÇÕES PORTUGUESAS?

O que digo aos meus clientes, numa primeira instância, e para aqueles que vão investir no modelo de segurança, é que há três pontos que devem ser

colocados na agenda de qualquer gestor de topo que tem um negócio no ciberespaço.

Na ótica da prevenção, é preciso focar na capacidade de se autoavaliar continuamente sem melindres e criar um modelo de autoavaliação constante, à procura de falhas – e não são falhas à procura de quem é que falhou; falhas para procurar como corrigir rapidamente. Não é com ações milagrosas, às vezes é com *quick wins*, com ações de mitigação do risco, mas tenho de saber qual é o meu *playground* de falhas. Baseado nisso, vou investir ali, ali e acolá e gerir o meu risco, mas com conhecimento de causa.

Na ótica do durante, é necessário implementar capacidades de monitorização e alarmística. É preciso ser capaz de montar uma estrutura que monitorize o meu negócio, a minha atividade digital 24 horas, sete dias por semana, à procura de ações erróneas, suspeitas ou maliciosas para conseguir encurtar o tempo da atividade criminosa na minha organização. É ganhar tempo, comprar tempo.

Os grupos criminosos hoje fazem ataques, fazem intrusão. A forma de fazer intrusão varia constantemente. Há um período oculto na rede em que estão a descobrir quem é quem na rede, onde estão os ativos, onde está o dinheiro. No fim, roubam os dados, depois apagam ou encriptam, ou até podem destruir tudo. Este tempo oculto é onde a minha capacidade, a minha guarda armada, vai detetar algo antes de roubarem ou destruírem. Hoje não é só uma tendência, é uma obrigação.

Se formos ver grande parte dos ataques destrutivos em Portugal e no mundo são feitos a uma sexta-feira às quatro da manhã e não é ingênuo. Eles sabem que não há guarda-armada àquela hora ou que os olhares estão menos atentos. Antes, este tempo oculto durava semanas; hoje dura horas, no máximo um dia ou dois. Temos de ser capazes de capturar estes momentos suspeitos, antes de haver algo mais violento.

Por fim, o após. Quando o dia chegar, estar preparado para me levantar. Preparamos continuamente os clientes para, que quando acontecer, tenha muito bem balizado o que fazer num processo em que foi vítima de um ciberataque ou de um ciberdesastre, em que sabe muito bem o que é que vou levantar, qual é a sala de crise, quem é que vai ter na sala de crise, quais são os mecanismos que vai acionar para se reerguer, com quem é que vai comunicar, como é que vai comunicar com o ecossistema de parceiros, fornecedores, clientes, autoridades de controlo, se tecnologicamente tem *insight* para conseguir levantar os sistemas novamente… tudo isto tem de estar testado em tempo de paz porque, quando houver um tempo de guerra, sei precisamente o que fazer e não há momentos de pânico ou de criatividade instantânea. Tem de ser muito bem parametrizado. Não quer dizer que os planos funcionem sempre – não vão funcionar –, mas temos balizas e temos um conjunto de alinhamentos muito bem definidos para que não haja grandes margens para decisões instantâneas ou muito criativas. ■