PUBLIREPORTAGEM

Há 15 anos em Cabo Verde

VisionWare lança centro pioneiro de análise de ciberameaças à segurança

Com uma carteira de clientes diversificada, entre o sector público e privado, fruto de uma presença sólida, há mais de 15 anos, no país, a VisionWare é hoje uma referência em matéria de segurança de informação em Cabo Verde. Bruno Castro, presidente do conselho de administração da empresa, esteve recentemente na Praia, para reforçar o acompanhamento aos clientes e apresentar o Threat Intelligence Center, um centro pioneiro de análise de ciberameaças à segurança mundial. Este centro permite agir por antecipação e aumentar a capacidade de resposta em matéria de cibercrime.

Bruno Castro, Presidente do Conselho de Administração

Qual o contributo que este Threat Intelligence Center vai trazer para a cibersegurança?

Na VisionWare trabalhamos ao nível de várias camadas, por assim dizer, relacionadas com o cibercrime. O cibercrime actua sobretudo no submundo da internet, e nós já fazemos, há vários anos, através da monitorização de redes e de grupos criminosos, da rede de comércio underground, onde se comercializa informação roubada, ou seja, na darkweb, deepweb, nos vários níveis de profundidade da internet.

Costuma-se associar a internet a um iceberg, em que a ponta que está fora da água é a internet, e tudo o que está para baixo é o submundo da internet, que é muito usado por terroristas, pedofilia, narcotráfico, armas, tráfico de pessoas, etc. Ou seja, há uma camada da internet, mais obscura, que é utilizada para suporte ao mundo do cibercrime.

Portanto, há muitos anos que monitorizamos esse submundo, a informação que está a ser roubada, como está a ser comercializada, ações programadas e como estão a ser executadas, mesmo ao nível de segurança física, de ameaças aos próprios Estados.

Há medida que tem havido mega-ataques, nós verificamos que temos de ter capacidade a dois níveis. O primeiro é preventivo, em que à data de hoje, temos de conhecer, por exemplo, se a informação de um cliente nosso já está a ser comercializada na darkweb por grupos criminosos, informação essa que será mais tarde utilizada para os atacar.

O segundo é reativo, ou seja, após um ciberataque, temos de saber exatamente que grupo cibercriminoso desenvolveu o ataque, como é que ele opera no cibercrime, que metodologia utiliza para atacar e comercializar o que rouba, para depois passar a informação às autoridades policiais, e simultaneamente, nos prepararmos para responder operacional e tecnicamente.

Devo notar que este centro conta já com cerca de 10 especialistas nas áreas de intelligence e cibersegurança, nos nossos escritórios no Porto e em Lisboa, incluindo também alguns operacionais do escritório da cidade da Praia, em Cabo Verde, através do nossos Security Operations Center. Ainda temos uma estrutura mais leve que opera através de uma parceria local na cidade do Panamá.

Este centro permite então reagir por antecipação?

Sim. No fundo, em suma, este centro faz a monitorização constante, de forma infiltrada, do que se passa nesse submundo da internet, para nos protegermos antecipadamente de um ataque e, posteriormente, podermos bloquear esse ataque e minimizar o impacto por antecipação.

Isto traz mais segurança?

Prefiro dizer que traz mais capacidade de resposta. Tipicamente, quando há um ataque, nós só sabemos que houve esse ataque após haver a destruição ou a disrupção de serviços. O tempo oculto de permanência na rede do cliente, às vezes, é seis, oito, dez semanas em que está escondido, de forma oculta, a monitorizar o que se passa na rede, a roubar informações para depois poder comercializá-las, e por fim, preparar o ataque de carácter destrutivo.

Se conseguirmos saber que alguém já está escondido na minha rede, a espiar ou a comercializar a informação que roubou, e a publicitar isso para o mundo do crime, eu vou poder reagir antes do grupo criminoso poder destruir e esta é a resposta que acaba por ser mais relevante. Por exemplo, o que aconteceu com a Vodafone e a SONAE, que ficaram sem comunicações, este tipo de acções já só sabemos na fase de desastre e o que nós tentamos ganhar de vantagem é precisamente o tempo de antecipação à fase destrutiva do ataque.

De Cabo Verde para o mundo

Estão em Cabo Verde desde 2007. Que balanço é que fazem da vossa presença no mercado?

Hoje posso dizer que "aterramos" em Cabo Verde por um golpe de sorte, na altura foi uma oportunidade de negócio. Fomos convidados pelo Banco Mundial de Investimento a concorrer a um concurso, ganhamos e acabámos por ficar até hoje. Passados 15 anos, estamos ligados à adminstração pública, central, às autoridades nacionais, ao sector financeiro, e na realidade, às principais empresas do sector privado do país.

Com o crescimento do merca-

do, criamos dois polos de operação em Cabo Verde, em que, a partir daqui, trabalhamos também para o mundo, com os nossos recursos técnicos cabo-verdianos, formados e coordenados por nós.

Algo que descobrimos ao longo dos anos, é que Cabo Verde tem matéria prima de recursos humanos muito valiosa. Quer ao nível da área da segurança, quer ao nível de formação técnica, mas mais importante, no que respeita o caráter humano que temos vindo a valorizar face a outras geografias onde operamos. A cultura de Cabo Verde é claramente um factor diferenciador.

Como marco do nosso investimento em Cabo Verde, posso confirmar que a nossa equipa de reação rápida, layer 1, que opera aqui, do Security Operations Center, trabalha para os nossos clientes espalhados pelo mundo.

Criaram o primeiro escritório na Praia e tencionam abrir no Mindelo, também. Isto é uma resposta à demanda do mercado?

Primeiro criamos uma estrutura operacional na Praia, há cerca de meio ano, e já estamos a trabalhar para aumentar essa equipa da capital. No próximo ano, estamos a trabalhar para criar, também, em São Vicente, um pólo com as mesmas caracteristicas operacionais.

Pela forma como fomos tão bem recebidos desde sempre, assumo que temos aqui uma "dívida" para com São Vicente e queremos fazer investimentos lá, também. Porque temos, igualmente, recursos humanos valiosos, vindos da nossa parceria com o NOSi Akademia ou diretamente das universidades, que são de São Vicente ou Santo Antão, pelo que faz algum sentido inseri-los na sua região.

Hoje, temos aqui, na Praia, pessoas que são de São Vicente e Santo Antão, que estão deslocadas e faz algum sentido esse reajuste para nós.

Neste momento, temos à volta de 15 pessoas no escritório da Praia e vamos aumentar esse número, claramente. Acredito que vamos chegar rapidamente às 30 pessoas na Praia. Em São Vicente iremos crescer devagar, mas perspectivo chegarmos a uma dezena, pelo menos, a curto prazo.

Disse atrás que trabalham a partir de Cabo Verde para o mundo. A demanda da procura pelos vossos serviços também tem crescido aqui?

Sim, mas na limitação da dimensão do mercado de Cabo Verde. Ou seja, eu diria que ao fim de 15 anos estamos presentes em quase todas as empresas privadas, nas principais referências do sector público e na própria administração central, porque temos uma presença muito sólida e presente desde 2007. Não temos uma área comercial e, na realidade, acabamos por ser chamados na "palavra puxa palavra", que é nossa preferência, tanto aqui, como em Bruxelas, Lisboa ou Porto, esse é o nosso modelo comercial em todas as geografias onde operamos.

Aqui em Cabo Verde é mais fácil, porque o mercado é mais pequeno e, portanto, as pessoas conhecem-nos mais rápido, em termos de referências, porque, mesmo trabalhando entre empresas concorrentes, as referências do nosso bom trabalho passa de forma horizontal entre as pessoas de cada instituição. Esta relação de compromisso está assente na confiança e qualidade do nosso trabalho desde há muitos anos. As relações de proximidade são a consequência desse compromisso, do nosso historial e da própria cultura de Cabo Verde.

Ao nível do Estado é precisamente o mesmo conceito. O facto de colaborarmos com o NOSi, até em modo de parceria, ao nível da rede do Estado, também nos dá essa relevância, num mercado que é pequeno, mas que também é exigente, e procura estar constantemente em evolução para os níveis do que melhor se pratica a nível internacional.

Eu não diria que há mais demanda, mas sim que há a demanda normal, especialmente numa altura, em que a cibersegurança é um tema quente, tanto aqui como na Europa, ou no mundo.

A par das melhores referências

Há um interesse de Cabo Verde em estar a par de tudo o que se faz lá fora nesta área, para estar preparado?

Claramente. Eu costumo dizer que Cabo Verde tem essa particularidade de querer estar na "curva da onda", ou seja, há uma procura constante por quererem estar referenciados, não com o que se passa no mercado africano, mas com o que se passa no mercado europeu. Procuram, de forma até irreverente, o que melhor se desenvolve no mundo. Essa ambição está precisamente alinhada com o DNA da VisionWare.

O que está acontecer é que o mercado está a evoluir muito rápido, especialmente, por exemplo, no controlo das autoridades a nível internacional que tem impacto direto sobre Cabo Verde e na sua relação com a Europa. Nesse sentido, quer o Estado, quer o tecido empresarial, nomeadamente aquele que se relacione com a Europa, terão que dar um salto qualitativo no que respeita o tema da cibersegurança de forma a poder pertencer a um ecosistema seguro a nível internacional. Estou convicto, até pelo que tenho assistido nos nossos clientes, acrescido da própria estratégia do Estado e do próprio NOSi que, aqui em Cabo Verde, irá acontecer precisamente esse salto qualitativo em termos de segurança cibernética.

Quais são os vossos principais projectos no mercado cabo-verdiano, pelo menos aqueles que podem divulgar?

A VisionWare não tem propriamente projetos. Fazemos parte da comissão de segurança dos nossos clientes, em modo residente, e com competências multidisciplinares, permitindo-nos apoiar continuamente nas vertentes de cibersegurança, compliance, privacidade, forense, etc. Estamos continuamente envolvidos em tudo que envolva a gestão de segurança dos nossos clientes, seja nos sector da banca, seguros, distribuição, farmacêutica, etc. Temos um modelo de operação de enorme proximidade com a camada de gestão e simultaneamente com as equipas operacionais na gestão "quase diária" dos desafios de segurança que nos são apresentados.

Podemos dizer que, hoje em dia, há uma maior preocupação da empresas cabo-verdianas em relação à cibersegurança?

Completamente. Quer da mensagem que passa do Estado, para baixo, porque eles próprios estão preocupados, e incutem isso nas empresas públicas, e, depois isso acaba por replicar para o sector privado. No entanto, também importa reforça que nos últimos anos, a própria gestão das empresas do sector privado, onde estamos residentes, já têm no seu mindset o tema da segurança e que têm de apostar nisso, rapidamente, e com força. É uma realidade deste novo mundo cibernético que os gestores, também em Cabo Verde, já estão completamente contextualizados sobre os desafios que se avizinham.

Isso tem a ver com a mediatização dos ataques que têm ocorrido a nível mundial?

Sim, em grande parte, deve-se, também, a isso. A esses ataques que têm acontecido em Portugal de forma tão destrutiva, e que têm passado para aqui, rapidamente. Portanto, há esse alerta global e Cabo Verde não está imune, e tem perfeita consciência disso.

PUBLIREPORTAGEM

Pessoas e empresas mais expostas

Maior maturidade

Cabo Verde tem algumas vulnerabilidades específicas nesta matéria de cibercrime?

Não vejo assim nenhuma grande diferença ao nível da exposição do risco. Os ataques que temos em Cabo Verde, temos em Portugal, Espanha ou Bélgica, por exemplo.

Mas, o que vemos aqui, é que, efetivamente, há ainda zonas imaturas, e nas quais é preciso investir, rapidamente, para se chegar a um nível de maturidade que seja o adequado. Não nos podemos esquecer que o cibercrime é global, não é regional. É tipicamente feito por sectores de actividade.

Temos grupos cibercriminosos altamente especializados, por exemplo, na indústria automóvel, na banca, nos seguros, na educação ou saúde. Para eles estar num hospital em Cabo Verde ou Lisboa ou Bruxelas é a mesma coisa, porque se focam nisso especificamente nesse sector.

Por isso, reitero que é mais uma questão de alguma imaturidade ao nível do fator humano, na necessidade de formação e consciência dos riscos por parte das pessoas.

Em Cabo Verde, hoje em dia, temos uma população muito digital, que gosta da internet e há um conjunto de serviços que o próprio Estado está a preparar-se para dar, digitalmente, e é preciso estarem preparados para estas questões de segurança cibernética. A transformação digital que o Estado pretende implementar e dessiminar culturalmente em Cabo Verde, irá trazer obrigações e desafios no que respeita a cibersegurança. É uma inevitabilidade.

Um dos projectos que têm com o Estado é a implementação da pulseira electrónica em Cabo Verde. Temos condições para isso?

Completamente. Cabo Verde está avançar, para estar em referência, nesta questão da segurança, ao nível do que se faz na Europa e noutras paragens. O Ministério da Justiça está apostar fortemente na vigilância electrónica. Estamos numa fase já muito avançada da implementação da pulseira electrónica, como, aliás, a própria Ministra da Justiça, Joana Rosa, já comunicou publicamente.

É um projecto que envolve tecnologia de ponta, serviços altamente especializados, formação de recursos humanos, é muito abrangente e complexo, é um facto. Estamos conscientes da exigência do desafio, mas posso confirmar que a pulseira electrónica será uma realidade que vai acontecer a curto prazo em Cabo Verde.

Esta questão da ciber-segurança também exige uma grande qualidade ao nível da internet. Como é que avalia Cabo Verde neste aspecto?

Ao final de 15 anos em Cabo Verde já passei por tudo. Já passei pela internet que era um luxo, até hoje, onde já é uma comodidade. Antigamente, para termos internet num hotel tinha-se que pagar e pagava-se uma fortuna para ter internet durante uns minutos. Hoje já temos infraestruturas bastante boas, onde a rede do Estado, assente no NOSi, é uma rede moderna, segura, bem equipada gerida por bons operacionais. Aliás, não me canso de dizer isso, que quer o NOSi, quer o Estado têm recursos muito bons tecnicamente.

Bruno Castro, Presidente do Conselho de Administração

O ciber-crime em Cabo Verde tem aumentado?

Tem aumentado na mesma métrica que temos sentido em todo o mundo. Nos últimos dois anos tem havido uma explosão do número de ataques e, pior do que isso, tem sido uma mega-explosão do número de ataques com sucesso. Esse diria que é o principal ponto a reter. A permeabilidade dos ataques realizados e o impacto que têm causado na sociedade moderna. Tem sido um tomar de consciência muito doloroso, especialmente, para a confiança que tinhamos na resilência das nossas infraestrutura críticas.

Temos mais alvos disponíveis?

Sim, claramente. Porque grande parte da população, devido à pandemia, passou a estar em teletrabalho, e, isto, também se transformou numa pandemia cibernética. Porque todos nós saltamos para a internet, os miúdos acabaram por ter aulas online, as pessoas ficaram em trabalho remoto e as empresas tiveram que abrir canais de comunicação para as redes domésticas dos seus colaboradores de forma quase instantanea. Houve uma grande percentagem de empresas que tiveram que recriar os seus negócios na internet porque fisicamente não era possível e, acabaram por perceber da pior forma, que não estavam ainda maduras o suficiente para estar na internet. Portanto, por estas todas razões, o cibercrime passou a ter muito mais alvos disponíveis, e pior que isso, vulneráveis.

As empresas passaram a estar mais expostas?

Muito mais expostas. E, pior que as empresas, as pessoas. Essa foi outra mudança abrupta que sentimos nos últimos dois anos. Foi o cibercrime endereçar grande parte do seu esforço inicial ao ataque sobre pessoas, para posteriormente, depois de comprometidas, as utilizar como trampolim para as suas organizações. O factor humano tem sido cada vez mais o nosso maior desafio em termos de segurança.

Nesse aspecto, têm serviços para as pessoas individuais?

Temos serviços que aplicamos a VIP´s, ou seja, pessoas e personalidades com exposição elevada ao risco, como políticos, empresáros, pessoas ligadas ao desporto, etc., em que temos serviços especializados para os proteger, na medida do possível, às ameaças digitais. É quase como um serviço de bodyguard digital.

Em Cabo Verde também têm esses clientes VIP´s?

Temos sim.

Solidificar e crescer

Quais as perspectivas de futuro em relação ao mercado cabo-verdiano?

Vamos continuar posicionados onde temos estado nos últimos 15 anos junto do Estado, assente muito na nossa parceria com o NOSi, e nas principais empresas do sector privado de Cabo Verde. Antevejo um forte investimento do Estado, ao nível da modernização e da consolidação da era digital, em termos dos serviços para o país, pelo que admitiria que também haverá uma forte preocupação do Estado em promover esses serviços digitalmente, e para a internet, de forma segura.

Por isso, haverá uma aposta da VisionWare em trabalhar, lado a lado, com o Estado e com o NOSi na promoção desses serviços online, com a imagem de qualidade e segurança que eles merecem.

Importa ressalvar que Cabo Verde é mais que uma segunda casa. A decisão da VisionWare em investir numa operação física a nível local, com colaboradores caboverdianos, não se prende pelo volume de negócios que temos aqui, mas sim, pelo capital humano que existe, pelas sustentabilidade das relações de parceria que criámos e, essencialmente, pela cultura de um país sempre nos tratou tão bem.

Ao final de 15 anos, sentimos que é óbvio que a estratégia de continuidade em Cabo Verde se irá manter e, numa perspetiva mais global, irá certamente crescer.