

CIBER-SEGURANÇA

Especialista alerta que Cabo Verde pode ser alvo de fraude bancária, roubo de identidade e violação de dados

» Bruno Castro, fundador da VisionWare, uma empresa de tecnologia especializada em cibersegurança, alerta que pela “juventude” do seu mercado digital, Cabo Verde pode vir a ser alvo de fraude bancária, roubo de identidade, violação de dados e até cyber-bullying. Apesar da confidencialidade a que uma empresa destas está sujeita, em entrevista ao A NAÇÃO, esse especialista fala dos projectos em curso no país e dos desafios que o arquipélago enfrenta na era digital.

■ Gisela Coelho

A NAÇÃO -A VisionWare celebra 10 anos de presença no mercado cabo-verdiano. Que balanço é que fazem da vossa actividade?

Bruno Castro - Desde a fundação (2005) que tivemos uma estratégia para a internacionalização, nomeadamente, nos PALOP, mas nunca imaginámos vir a centrar a nossa actividade em Cabo Verde. Só quando ganhámos o concurso do Banco Mundial de Investimento para o Banco Central de Cabo Verde é que avaliamos o potencial do mercado e a possibilidade de estender operações. Ainda bem que o fizemos. Fomos muito bem-recebidos, ou não fosse a “morabeza” deste povo que tanto nos tem ensinado. São 14 anos de uma decisão estratégica sustentável que, rapidamente, passou a emocional, com excelentes resultados e referências em tudo semelhantes a Portugal e Europa. Estou convicto que continuará a ser um sucesso.

Em que áreas é que têm atuado, sobretudo?

Temos atuado em todas as áreas, já que a “segurança” se apresenta como uma necessidade transversal, cada vez mais crítica. Destacamos a nossa colaboração com a Administração Pública (Justiça e Autoridade), Energia, Transportes (Aéreo e Marítimo), Banca & Seguros. Sectores onde detemos uma longa experiência em Portugal, Europa e

Médio Oriente.

Quais os principais projectos que já desenvolveram?

É difícil indicar um projeto principal entre os restantes, ainda para mais dada a forma intensa, proativa e exemplar – face a outras geografias onde operamos - com que o mercado de Cabo Verde tem aderido aos nossos serviços e ao tema da “segurança”. Encaramos cada cliente, privado ou público, mais pequeno ou maior, com a particularidade que lhe é devida, adaptando-nos às suas necessidades. As colaborações que temos tido levam-nos a assumir que contribuímos para o incremento do nível de maturidade de segurança de Cabo Verde, o que nos deixa bastante satisfeitos.

Daria três referências: o nosso primeiro projeto (2007) - a referida auditoria de segurança e definição do modelo de segurança do Banco Central, relevante pela sua importância e por ter sido o mote para estarmos hoje “residentes” no país.

Depois, o processo de certificação na norma internacional de segurança de informação – ISO/IEC27001 – da Caixa Económica de Cabo Verde (2012), que, até hoje é a única instituição bancária certificada nesta norma no mercado PALOP.

E, por fim, ainda em curso, a parceria estabelecida com a Polícia Judiciária de Cabo Verde (e outras polícias europeias) no âmbito de um projeto europeu de enorme relevância para a evolução da tecnologia de vigilância eletrónica que irá



apoiar futuros processos de investigação criminal na Europa e em Cabo Verde.

Quais os projectos que têm em curso, actualmente?

Pela sensibilidade e confidencialidade da nossa área posso apenas referir que temos apostado em projetos de carácter continuado, relacionados com a implementação e posterior governação no tema da (ciber) segurança; certificação ISO/IEC27001; e, mais recentemente, no tema de privacidade de

dados pessoais face à adesão de Cabo Verde ao Regulamento Geral de Proteção de Dados. A nossa equipa é Lead Auditor e Lead Implementer, consultora na definição de processos de evolução e maturidade tecnológica e aplicacional nas organizações e apoio em ações de investigação forense, após fraude, incidente de segurança ou crime.

Quais têm sido os vossos principais clientes/parceiros?

Conforme referi, não quero

identificar os nossos clientes – já muitos e de “longa data”. A grande maioria está connosco há mais de 6 anos e integra os setores público e privado.

Mercado digital “jovem”

Como têm visto o desenvolvimento da cibersegurança no mercado cabo-verdiano? É um mercado ainda incipiente?

A evolução do tema da (ciber)segurança tem sido reflexo da enorme vontade de acom-

panhar as tendências globais, sendo que Cabo Verde se tem destacado de forma bastante positiva, face ao restante mercado africano. O incremento substancial dos utilizadores com acesso à Internet, assim como a adesão global dos serviços estatais e empresariais ao mercado cibernauta, obriga a grandes adaptações e ajustes até que o mercado “digital” em Cabo Verde possa ser considerado maduro em segurança de informação. Pela sua “juventude”, estamos convencidos que irá ser um alvo de ataques como fraude bancária, roubo de identidade, violação de dados - informações confidenciais governamentais, empresariais e pessoais.

O que fazer para evitar isso, quer as entidades públicas, quer as empresas e o cidadão comum?

Primeiro, apostaria na tomada de consciência do tema da segurança e das ameaças que existem, actualmente, no mundo da cibersegurança por parte de todos. Depois, depende. As exigências de uma entidade governamental ou financeira são diferentes das de uma empresa de menor dimensão ou criticidade. Há que iniciar a implementação de um modelo de governação de segu-

rança nas suas dimensões física e lógica. Consoante a correta avaliação do actual nível de segurança interno – através de uma auditoria transversal – é então necessário definir prioridades para minimizar o risco. Cada caso terá os seus padrões de gestão de risco e medidas preventivas/corretivas a implementar, coerentes com as respetivas exigências e nível de maturidade. É um processo a longo prazo, contínuo, a abordar pela gestão da organização. Nesse fórum, os decisores deverão conhecer do risco, ameaças e decisões a tomar, daí em diante, para proteger a sua organização.

O que falta a Cabo Verde para avançar no domínio da cibersegurança?

Desenvolver a cultura de (ciber)segurança para responder às exigências de alguns setores governamentais e empresariais que irão, forçosamente, ter de cumprir standards internacionais bastante mais exigentes do que os praticados no mercado local. De resto, pelo que conheço de Cabo Verde, não tenho dúvidas de que responderá atempadamente aos riscos de segurança existentes e, aí, a própria cultura de segurança da comunidade evolui-

rá drasticamente. Existem já casos de ataques com sucesso em Cabo Verde que servirão, certamente, para alertar os decisores governamentais e empresariais deste país, para que desenvolvam medidas proativas, alterando o panorama a curto prazo.

Que desafios enfrenta Cabo Verde ao nível da cibersegurança?

Os mesmos desafios que qualquer outro país conectado ao mundo cibernauta. Tomar consciência da importância da salvaguarda da informação (pessoal e corporativa) é essencial. A internet, a digitalização, a globalização, trouxeram um conjunto de oportunidades a todos os países e suas organizações, empresas e indivíduos. Mas também trouxeram um conjunto de desafios para a segurança de quem “lá vive”. Hoje, as ameaças vão além da segurança física. São também digitais e, mesmo estas, podem interferir com a segurança física dos seus intervenientes. Estamos a falar de ataques como ciberterrorismo - ataques em infraestruturas críticas (energia, água, comunicações, transportes); violação/

roubo de informação ou de identidade, fraude bancária, extorsão e pedido de resgate, cyberbullying, entre outros.

Data Center Praia e São Vicente

Que papel é que podem ter o Data Center da Praia e do São Vicente (em construção) nesse domínio da cibersegurança?

São um sinal da evolução na maturidade tecnológica de Cabo Verde e espera-se que promovam enormes mais valias no domínio da segurança de informação. A sua manutenção e segurança, trará desafios no estabelecimento de um nível de segurança adequado às suas funções, em particular, na implementação de medidas de segurança digital e física. Estou convicto que Cabo Verde responderá positivamente.

Cabo Verde tem servido de plataforma para a Visionware entrar no Mercado da cibersegurança da sub-região Africana?

A relação que temos com Cabo Verde é muito especial. Fora de Portugal, além de Bruxelas, apenas temos residência em Cabo Verde - Santiago, São Vicente e Sal. Mas não diria

que esse foi um factor para entrar comercialmente em outras geografias. Estranhamente, os casos de sucesso em Cabo Verde não são bem aceites noutros países africanos. Pelo contrário, são mais reconhecidos na Europa. É prova disso a recente aceitação da proposta da VisionWare à Comissão Europeia: levar a Polícia Judiciária de Cabo Verde a participar num projeto de investigação e desenvolvimento de tecnologia avançada quando os membros são tipicamente entidades europeias.

Quais são os projectos que têm em carteira para o futuro no país?

Além dos projetos de carácter continuado como “security officer” residente, os próximos desafios onde a VisionWare é especialista, implicam o Regulamento Europeu de Proteção de Dados Pessoais, a que Cabo Verde aderiu no ano passado, em Bruxelas. Tem sido um desafio para todos os países aderentes desde que entrou efetivamente em vigor (2018) pelo que será também para Cabo Verde. Recordo que tal obriga a um nível de maturidade em (ciber)segurança, conformidade ISO/IEC27001, além da componente legal. A grande maioria não está preparada... Cá estaremos! 

Perfil

Licenciado em Engenharia Eletrotécnica pela Faculdade de Ciências e Tecnologia da Universidade de Coimbra, onde obteve o grau de Mestre em Engenharia Informática (Segurança Informática), Bruno Castro foi um dos fundadores da VisionWare em 2005. Concluiu o MBA em Gestão de Empresas, na Escola de Negócios EUDEM (em associação com diversas escolas de negócios internacionais). Antes de fundar a VisionWare, construiu a sua carreira

profissional na Critical Software, WhatEverNet, Novabase Consulting, e Quatro, participando ainda em várias comunidades, nacionais e internacionais, de Segurança Informática. Desde a fundação, tem participado activamente na concretização da estratégia de internacionalização da VisionWare, nos continentes europeus e africano, e na consolidação do posicionamento da empresa junto da Comissão Europeia, traduzida na participação nos projetos FOREN-

SOR, CYSPA e LASIE. Foi responsável pela gestão de um projeto NATO, classificado como SECRETO, junto do Ministério da Defesa da Argélia. Está credenciado NATO-SECRET e Nacional Secretário de Defesa da Argélia. Está credenciado NATO-SECRET e Nacional Secretário de Defesa da Argélia. Faz parte do grupo de auditores de segurança credenciado pelo Gabinete Nacional de Segurança (Portugal). É membro do IAPP – The International Association of Privacy Professionals, a maior associação internacional de Profissionais a atuar na Área do Privacy e

da Proteção de Dados.

A VisionWare é uma empresa tecnológica especializada em cibersegurança, que se dedica à comercialização, desenvolvimento, manutenção e prestação de serviços de auditoria, consultoria, implementação e gestão de plataformas tecnológicas associadas à componente de segurança de informação. Hoje é uma referência no sector da segurança informática e protecção de dados, com projectos ligados à EU e NATO. GC



“...em **Cabo Verde** há mais de **10 anos!**”
vemos o que você não vê

www.visionware.pt