Economia

Entrevista – Bruno Castro

Ataques informáticos vão aumentar em Cabo Verde

Bruno Castro é o director-geral da VisionWare, empresa portuguesa que trabalha na área da segurança informática e todas as suas envolventes, desde intrusão, investigação, auditoria de soluções, auditoria de infra-estruturas ou certificações. Estão em Cabo Verde há cinco anos, onde operam para o governo, para a banca e para instituições privadas. O próximo passo é fazer do arquipélago a base para exportar serviços para os PALOP e para o Brasil.

Entrevista Jorge Montezinho | Fotos Quim Macedo

D o que falamos quando nos referimos à segurança informática?

A segurança informática é tudo. Desde enviar e-mails a estar sobre escuta, tudo isso é segurança. Tudo o que fazemos hoje está envolvido por essa redoma de segurança. Por exemplo, todo o conceito de segurança do passado, paredes, portas, etc., hoje tem a mesma relevância, mas em termos virtuais. Dantes, íamos ao banco levantar dinheiro, ou tínhamo-lo num colchão. Hoje, fazemos tudo pela Internet, sejam depósitos sejam transferências. Em termos de negócios, é a mesma coisa. Hoje, o paradigma é tudo o que fazias no mundo real, hoje fazes no mundo virtual, numa analogia directa um para um. Quem não estiver nesse mundo, está a correr riscos a nível pessoal e a nível empresarial. A insegurança informática é uma realidade, não há forma de a contornar. E nós somos chamados para tudo, desde processos crimes até à área militar por causa do ciber-terrorismo. Aliás, este é um bom exemplo, tal como põem bombas, os terroristas hoje também tentam furar os sistemas informáticos. Imagina que entram, digamos, numa fábrica que faz medicamentos para crianças. Basta alterarem a composição dos remédios, converterem-nos em veneno e está dado o golpe.

E o cidadão comum, que não tem empresas, como se protege?

Nós começámos a trabalhar via empresas e via governo, mas hoje há essa questão, a do cidadão comum que navega na Internet. O elo mais fraco é sempre a parte humana. Mesmo numa empresa, com regras fortes e com sistemas complexos de defesa, há sempre um ser humano por trás, a trabalhar, e que erra. Em casa, quando vais à Internet, normalmente, és alvo de fishing. Recebes um mail, a dizer que é o teu banco, e não tens forma de saber se esse mail é real ou não. Mesmo as tuas fotos, as tuas informações pessoais, que hoje toda a gente guarda no computador, são alvos procurados. Numa empresa, temos maneira de nos protegermos, corporativamente. E hoje, de facto, a preocupação são as pessoas, a começar pelas crianças. Há uma situação muito sensível, e que aparece cada vez mais, que é o uso do Messenger, de chats e do facebook pelas crianças. Este é um problema grave. Geralmente, as crianças dominam mais a informática que os pais, logo, os pais partem em desvantagem, e ao usarem estas ferramentas, as crianças não sabem quem está do outro lado. Nós, como pessoas que trabalhamos na área de segurança, que temos a obrigação de proteger, temos sérias dificuldades e é um dos grandes desafios que temos hoje na União Europeia, como proteger o cidadão vulgar. Porque não temos meios de entrar nas casas de todas as pessoas para ensiná-los. Monitorizar toda a Internet é impossível. Portanto, é um trabalho muito difícil. Mesmo convencer os pais que os seus filhos têm alguém do outro lado que eles não conseguem avaliar. Se ensinamos os nossos filhos a não falar com estranhos na rua, temos de os ensinar a fazer a mesma coisa na Internet.

E essa mensagem passa?

Não passa. É muito complicado. Estive, há uns tempos, num fórum sobre estas matérias, em que um dos inspectores me disse "o que eu fiz foi muito simples, pus o computador da minha filha no corredor. Assim, saiu do quarto, onde eu não conseguia controlar". E eu pensei, isto é mil vezes melhor do que qualquer técnica que eu tenha e que não garante esta protecção. Isto para nós é de facto um problema maior.

Bruno Castro, Director-Geral da Vision Ware

E que outras ameaças enfrentam?

O fishing. Mails enviados em nomes de bancos a dizer ponha aqui a sua password e as pessoas fazem-no.

Mas há assim tanta gente a acreditar nesses mails?

Imensa. E a banca hoje já estipulou que não suportará mais acções financeiras sobre isso, ou seja, passa o ónus para o utilizador. Dantes, o banco assumia parte, hoje não. Quem recebe um mail de fishing em casa é responsável por ele, por averiguar a sua veracidade, etc. Os bancos têm feito várias acções pedagógicas, a avisarem as pessoas para esta ameaça, mas mesmo assim há ainda imensos casos destes.

Voltando um pouco atrás, à questão das crianças usarem a Internet sem controlo, parece-me também que por vezes, são os próprios pais que não estão para se aborrecer.

Também é verdade. Há aqui dois grandes factores: há aquela mentalidade 'nunca me aconteceu nada, não vai ser agora', e as pessoas nem imaginam a ameaça que correm, e aqui, a falha é das próprias empresas de segurança que não avisam que as ameaças na Internet funcionam como as ameaças no mundo real. O outro factor é que se vais na rua e vês alguém que não te inspira confiança, reages. Na Internet isso não acontece. E se já é complicado, na vida real, dizer às pessoas para terem cuidado, trancarem bem as portas, avisarem a polícia quando vão de férias, na Internet é muito mais complicado. E os pais, muitas vezes, nem sabem o que é a Internet, que tem um lado negro, onde os perigos existem. Tudo isso torna muito complicado passar a mensagem.

É quase um contra-senso. A Internet é o veículo hoje prioritário para passar mensagens, mas não conseguem passar mensagens sobre a Internet.

É verdade. Mas a razão é porque andámos muitos anos preocupados com a segurança do mundo real, ganhámos desconfianças, intuições. Na Internet, no mundo virtual, ainda não. E em Portugal já vemos muito isso, muitas ameaças, ataques pessoais, seja para roubar informação, seja fotografias. E há casos, muitos, de exposição pública na Internet. E aqui, por exemplo, a forma de nos protegermos até é simples, basta não mandar o computador para arranjar com informação pessoal lá dentro. Quem garante que quem está a arranjar a máquina não está a aceder a informações? Fotografias? Aos e-mails? Quem o garante?

A informação vale hoje muito dinheiro.

Mas mesmo muito dinheiro. Acho que as pessoas não fazem ideia dos valores que estão envolvidos.

Redes Sociais

O fenómeno das redes sociais, em que alterou o vosso trabalho?

(risos) A nível empresarial e institucional, mudou pouco. O que mudou foi em termos das pessoas mediáticas, que têm o seu facebook ou outra rede qualquer, a quem avisamos sobre como devem proceder. Aliás, quem usa uma rede social tem de estar preparada para expor a sua vida, ponto. Seja uma pessoa anónima, seja uma pessoa conhecida. Tem de saber que está a colocar a sua vida na Internet e que essa vai ser acedida por quem entender. As redes sociais são engraçadas, funcionam muito bem, encontramos colegas de escola que já não víamos há anos, mas tem um lado bom e um lado mau. Temos problemas, muitas vezes, com figuras públicas, quando se expõem de mais, porque há sempre quem vai usar essa informação, sejam as pessoas que aparecem nas fotografias, sejam as poses menos próprias. Há imensos cenários que preocupam e o nosso papel aqui é pedagógico. Desencorajamos as figuras públicas a terem esses perfis, mas quando o fazem, pelo menos avisamos que tenham cuidado. A nível dos anónimos, têm de ter o mesmo cuidado que têm a gerir o seu Messenger, o seu e-mail pessoal. Quando metem um perfil no faicebook, essa informação pode ser usada por quem quiser, da maneira que quiser.

Aliás, ninguém sai do faicebook, a informação mantém-se.

É um passo em frente para o não retorno.

O conceito de privacidade. Vocês também se debruçam sobre ele? Afinal é algo que mudou, dantes estava dentro de quatro paredes e hoje está no mundo virtual, a vossa empresa também se preocupa com estas questões?

Preocupa, claro. A questão da privacidade é dúbia, porque é diferente da protecção de dados. São fronteiras bem definidas. Na protecção de dados há um suporte legal e este pouco varia de país para país. Privacidade é diferente, vai desde a exposição numa rede social, até ser alvo de vídeo-vigilância num posto de trabalho. Há um mito que diz que tudo o que se passa na Internet é vigiado, uma espécie de 'Big Brother' por cima disto tudo. Tenho dúvidas, mas é verdade é que há formas de monitorizarmos o que se passa nas redes que existem. Eu diria que o nível de privacidade é diferente do que era há uns anos atrás. Há países onde um mail não é privado. Por razões de segurança de estado, e por causa do terrorismo, há autoridades que vigiam o tráfego da Internet, mas não é global e só existe em alguns países. Em Portugal, por exemplo, isso não é permitido.

E cabo Verde? Como funciona em termos de legislação?

Penso que segue a legislação portuguesa. Tenho, aliás, boas experiências em Cabo Verde, é mesmo um 'case study' para nós, que trabalhamos na Europa, no Médio Oriente, em África. No mercado cabo-verdiano já se nota que há uma preocupação com a segurança e o risco, com o mesmo nível de rigor dos países mais avançados. Hoje, não vejo qualquer diferença entre um banco cabo-verdiano e um banco português. O país já começam a orientar-se por normas muitas rígidas, tanto mais que grande parte delas são normas internacionais. E há já uma consciência forte, tanto dos gestores como dos governantes, para esta matéria. Não diria que é em todo o Cabo Verde, mas já há uma grande preocupação.

Qual foi a mudança de paradigma a que se assistiu?

Entre 2000 e 2005 não houve grandes investimentos em termos de segurança, funcionava tudo na base da confiança, e em Cabo Verde, que é país pequeno, quase toda a gente se conhece. Mas, o outro lado é o abuso de confiança, e se quando entrámos cá toda a gente trabalhava assim, na base da confiança, hoje é diferente.

E se o país quer abrir-se ao mundo tem de tomar precauções.

Sim, estamos a falar de normas internacionais, como já disse. Hoje, o sector financeiro

cabo-verdiano disponibiliza serviços que não tinha há cinco, seis anos, e tem de garantir que esses serviços são de confiança. Hoje, já trabalhamos a um ritmo igual ao português, e já trabalhamos melhor, às vezes, do que em Portugal.

Ataques informáticos em Cabo Verde

Em Cabo Verde detectam muitos ataques?

Antes de mais, há vários níveis de ataques informáticos. Há o ataque informático que é meramente massivo, sem propósito, por exemplo, um vírus que anda na Internet a atacar tudo e todos sem mais objectivos. E isso há em Cabo Verde como há em todo o mundo. O que nos preocupa são os ataques com fim à vista, esses é que são os perigosos. Ou seja, quem acede a bases de negócios de empresas para passar essa informação para a concorrência, alguém que consegue aceder aos ficheiros pessoais, alguém que consegue apagar informações, ou pôr em baixa um negócio. Esses são os ataques cirúrgicos, rápidos, silenciosos, e geralmente quem está a atacar sabe o que está a fazer. Sabe onde tem de ir, onde tem de operar ou o que tem de destruir. Quando sai, apaga os rastos e, de preferência, incrimina alguém. A nossa função é sermos capazes de detectar esse tipo de ataques, se possível proteger preventivamente, senão proteger reactivamente, e se não conseguirmos mesmo proteger, temos de descobrir quem o fez e como o fez.

Como têm operado em Cabo Verde?

Geralmente, temos sido chamados para descobrir quem fez os ataques, porque houve casos em que quando entrámos o ataque já tinha ocorrido. Em Cabo Verde, os ataques mais detectados são os que envolvem acesso à informação, ou seja, alguém rouba informação que não é sua para benefício próprio, esse é o caso mais típico. Nos processos de investigação que tivemos, descobrimos sempre como foi feito, nem sempre descobrimos quem fez por uma questão muito simples, as empresas não estão preparadas, não têm uma espécie de 'caixa negra' que registe todas as evidências desse espaço temporal. Portanto, nem sempre dizemos quem o fez, mas descobrimos como o fez. Nas empresas e instituições com que estamos a trabalhar já instalamos sistemas que nos permitem ir atrás dos atacantes, ao mesmo tempo que protegemos a organização.

Mas as ameaças vão aumentar, não?

Sim, à medida que estamos a criar cada vez mais serviços online. O estado, a banca, as empresas, todas estão a entrar na Internet, e por isso, eu diria que as próximas grandes ameaças que vamos ter em Cabo Verde passarão por fraudes, por ataques a empresas para porem em causa a sua imagem. Como já temos em Portugal. Assim que pomos um serviço online somos logo bombardeados com ataques, desde fraudes, até tentativas de fazer correr em baixa a aplicação, alteração de sites, o que também vai ocorrer em Cabo Verde, e põe em causa a imagem da empresa. Imagina que isto se passa num banco, as pessoas pensam logo 'vou pôr dinheiro num banco que nem consegue proteger a sua página?'. Esta será a próxima ameaça em cabo Verde, ataques direccionados aos negócios.

Cabo Verde como base para os PALOP

Qual é o vosso mercado em Cabo Verde?

Vasto. Desde o governo, a banca, empresas diversas, quase todos os dias somos solicitados.

E qual é a estratégia de penetração no mercado?

Sinceramente, passamos de boca em boca. Não temos nenhuma estratégia comercial agressiva, temos boas referências e é assim que chegámos cá. Aliás, tínhamos ideia de montar uma sede em Luanda e agora vamos antes estabelecer-nos cá e daqui partir para o mercado dos PALOP. Temos uma base instalada já muito boa, com bons resultados tanto internos como externos e queremos continuar a crescer. Temos pessoas bem formadas, e apostamos em funcionários cabo-verdianos.

Estão também a pensar entrar na costa oeste africana, uma vez que Cabo Verde também pertence à CEDEAO?

Ainda não. Neste momento, os objectivos são mesmo Angola, onde já estamos com um volume de negócios bastante importante. Mas, como disse, Cabo Verde será a nossa casa para o mercado dos PALOP – Guiné e Moçambique, e também para o Brasil. Por razões muito simples: a parte geográfica, estamos a três horas do Brasil, a quatro de Angola e a quatro de Portugal. Depois, aqui temos uma massa crítica fantástica, temos vários cabo-verdianos que trabalham connosco em projectos internacionais e são óptimos. E finalmente, a estabilidade política e social de Cabo Verde também nos levou a querer ficar cá em vez de ir para Angola.

Para terminarmos. Objectivos a curto/médio prazo?

Criar em Cabo Verde uma base sólida que possa responder a todo o mercado cabo-verdiano e que nos dê capacidade de exportar serviços a partir de Cabo Verde, e isso para nós é muito importante. Em vez de estarmos a vender serviços a partir de Portugal para Angola ou para o Brasil, queremos fazê-lo daqui.