O ciberpolícia

A Visionware é como uma espécie de CSI da informática, sempre de olho em quem prevarica no meio digital. Combate o cibercrime, mas ganha dinheiro com ele

Parece um negócio tirado de um filme de James Bond. Antes de mais, por ter a confidencialidade associada à sua principal actividade: a consultoria e auditoria em segurança informática. É que a Visionware, como trabalha directamente com as autoridades policiais, tribunais ou até mesmo a Procuradoria Geral da República – como seus clientes ou em parceria –, participa frequentemente na investigação de muitos dos casos mais mediáticos da Justiça portuguesa, envolvendo a vertente informática, telecomunicações, escutas e afins. "O caso mais recorrente na área da segurança informática são ataques internos nas organizações, tais como fuga de informação, roubo de base de dados e outros", diz à INVEST Bruno Castro, o CEO da empresa.

É o exemplo daquele típico funcionário que, ao sair da empresa onde trabalhava, rouba dados confidenciais por via digital, para facultar à concorrência. E é aqui que entra a Visionware, cuja actuação começa no contacto com a cúpula da empresa (ou organização) que recorre aos seus serviços. A empresa apresenta depois à administração do cliente o nível de risco de segurança que essa organização incorre. Este é um processo contínuo que antecede a definição de um plano de correcção e mitigação do risco, em que se cruzam a matriz de risco e de investimento – por exemplo, se numa organização forem identificados 30 riscos, terá de saber quantos são de nível elevado para chegar ao valor do investimento que terá de fazer.

Só com este trabalho feito é que o cliente recorre a terceiros, no mercado, para a execução do plano de correcções – designam-se por integradores, que podem ser empresas nacionais ou internacionais das mais variadas áreas (sobretudo software, hardware e/ou serviços). "Durante a execução do plano, controlamos e avaliamos a sua aplicação, para nos certificarmos que o problema foi resolvido", explica o responsável, formado em engenharia electrotécnica, que fundou a Visionware há seis anos, com um grupo

Visionware

• 2 formas de actuação: avalia continuamente os riscos de segurança do cliente (auditoria) e desenha os processos de correcção contínuos para mitigá-los (consultoria).
O interlocutor é sempre o decisor – a camada de gestão, que podem ser presidentes do C.A., administradores, directores-gerais, etc.

• Investimento inicial (2005): 250 mil € (pay-back em 2006)

• Volume de negócios 2010: 2 milhões €
Cresceu entre 12% e 14% desde 2006, que prevê manter em 2011

• N.º colaboradores (consultores e auditores de segurança): 40

• Escritórios: Leça do Balio (sede), Lisboa, Viseu e Cabo Verde (2)

de amigos, no Porto. Em 2007 mudou a sede para o Centro Empresarial da Lionesa, em Leça do Balio.
Na prática, a sua tarefa pode ser preventiva – na detecção de falhas de segurança e potencial de risco dos clientes – ou reactiva, quando é chamada para investigar e resolver um incidente, desde um simples roubo de identidade electrónica até à maior fraude informática de impacto global. Enquanto especialista em intrusão, a empresa é multifacetada – faz a monitorização e testes constantes aos sistemas, desenvolve armadilhas para o combate a ataques e ameaças de segurança e colabora directamente com as autoridades nos processos de investigação forense. Em suma, ajuda a apanhar os ciberterroristas – os criminosos do mundo digital.

Actividade certificada

No sector privado, a empresa trabalha desde as empresas cotadas às PME e área financeira, sobretudo a banca. Mas tem clientes também na Administração Pública e na área da Defesa – ministério e serviços de autoridade. Para isso, está certificada pelo Gabinete Nacional de Segurança e monitorizada pelo SIS, que lhe dá a possibilidade de "trabalhar a matéria sensível do Estado português", admite o empresário.
Embora aposte nas certificações técnicas internacionais dos auditores, Bruno Castro aponta a dificuldade em encontrar colaboradores pela vertente humana. "Um auditor neste segmento da segurança tem de ter um perfil muito específico: pragmático, frio e com capacidade de resistir à pressão psicológica", descreve. Há ainda a componente do historial pessoal e familiar, sendo que são investigados os parentes directos do profissional a recrutar.
Para além da vertente técnica (intrusão), a Visionware dedica-se ainda, e desde 2007, à de compliance, a certificação de segurança obrigatória dos sistemas informáticos das organizações. Em Portugal, são os únicos a operar nas duas áreas – as auditoras financeiras concorrem no compliance, mas falta-lhes o know-how na área técnica – e fazem-no sob as normas internacionais da matéria. "Fazermos tudo o que diz respeito a segurança informática diferencia-nos no mercado:", sublinha o gestor. E trabalham ainda em projectos de segurança ao nível das Nações Unidas ("NATO Secret").
Operar lá fora, na realidade, está na génese da empresa. A aspiração de vir a ser uma referência internacional na sua área começou logo após o primeiro ano de actividade. O negócio doméstico foi replicado em Cabo Verde, escolhido por razões geográficas – num ponto estratégico entre a África, Europa e América do Sul –, mas também por ser um país organizado, estável e inovador. Mais uma vez, o perfil dos seus habitantes também ajudou: "Têm um potencial humano qualificado e de qualidade". A operação que lá montou – com três pessoas em dois escritórios – actua em todo o mercado dos PALOP, com clientes em Angola e abordagens mais recentes em Moçambique, Guiné e São Tomé.
Agora segue-se o Médio Oriente, um alvo em curso desde o ano passado, na área da Defesa. A ideia é entrar no mercado através de consórcios internacionais, nos quais a Visionware entre na segurança informática. De resto, a empresa já participa, desde 2007, nos grandes grupos privados europeus na área de segurança.
Sobre o sector onde opera, Bruno Castro lamenta que a maioria das empresas portuguesas ainda veja a segurança informática como um mero instrumento de trabalho, ainda que o grosso da sua actividade dependa dela. E justifica: "Há falta de conhecimento e percepção dos decisores em dar a real importância à vertente informática" – desde aplicações, bases de dados, sites institucionais, contas de e-mail, informação sobre clientes, pricing e outros. Por isso, revela, é recorrente "sermos chamados para casos em que todo o negócio já está a «arder»".

Pedro Aleixo Pais