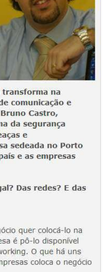
TDSnews
newsletter de inteligência económica das tecnologias de defesa e segurança

LÍDER

85% das grandes empresas portuguesas sem segurança



A Visionware, empresa portuguesa líder em soluções tecnológicas e aplicacionais nas áreas de segurança de redes e sistemas de informação, sistemas corporativos e gestão de plataformas T1/S1, surgiu como projecto de spin-out das maiores empresas, com reunião de um conjunto de especialistas na área de segurança. É a única empresa credenciada pelo Gabinete Nacional de Segurança, o que a transforma na referência nacional em matéria de segurança de comunicação e redes. Numa entrevista exclusiva à TDSNews, Bruno Castro, administrador da Visionware, traça o panorama da segurança informática em Portugal, fala das maiores ameaças e vulnerabilidades e do contributo que a empresa sediada no Porto tem dado e vai continuar a dar para tornar o país e as empresas mais seguros.

Como está a segurança informática em Portugal? Das redes? E das utilities?

Actualmente, qualquer empresa que tenha um negócio quer colocá-lo na Internet, o primeiro passo após ser criada a empresa é pô-lo disponível para toda a gente. Isto envolve o conceito de networking. O que há uns anos era um luxo, neste momento, já 70% das empresas coloca o negócio fora de portas.

O que acontece é que, no dia em que coloco o negócio fora de portas, estou a disponibilizá-lo a uma entidade a que chamamos "selva" e está disponível a pessoas com intenções lícitas e ilícitas.

O EXEMPLO SONAE

Se pensar que tem um negócio seu, com um conjunto de bases de dados de clientes, facturações, de assets que não podem ser partilhados com toda a gente e está a disponibilizá-los na Internet, uma das coisa que tem de garantir imediatamente é que esse acesso é seguro, por duas razões: primeiro porque protege o seu negócio e segundo, porque legalmente é forçado a isso, quando coloca dados sobre os seus clientes na Internet é obrigado a segurá-los. Se houver uma fuga, a responsabilidade é de quem disponibiliza o acesso dados. Daí o conceito de networking ser hoje crucial.

Lembro-me por exemplo da banca e, por exemplo, do grupo Sonae para quem a segurança é fundamental, com um budget perfeitamente definido para essa área.

Mas, podemos dizer que hoje existe segurança informática em Portugal?

Não, ainda não. Podemos dizer que existe um conceito de segurança informática em 15% das grandes empresas portuguesas, as restantes estão a dar um primeiro passo nesse sentido, por duas razões: ou porque são obrigadas pelos clientes ou porque já sofreram com a falta de segurança.

Quais são, no seu entender, as principais ameaças e vulnerabilidades?

Diria que a maior ameaça hoje em dia é o roubo de informação associada a ataques à imagem. É comum haver roubo de informação em termos competitivos – e estou a recordar-me de algo que tem acontecido nos últimos meses com algum enfoque e que são os roubos internos, ou seja, pessoas que saem das empresas e levam bases de dados de clientes para empresas da concorrência, isto tem sucedido sistematicamente, e esta será talvez a principal razão para se falar nas empresas de segurança da informática – mas, a maior vulnerabilidade é a colocação do negócio na Internet.

De que modo é que a Visionware está e pode contribuir para melhorar este cenário?

Neste caso é a nossa abertura que está em causa. Tipicamente colocamo-nos do lado do cliente. Não temos, numa primeira fase, qualquer interesse em saber quais são as tecnologias em utilização. Só importa conhecer muito bem o modelo de negócio, saber o que é que transaccionam, o que precisam segurar, o que é crítico ou menos crítico, o que querem colocar fora de portas e dentro, quem acede... isto é que é importante. A partir daí, montamos estruturas tecnológicas, aplicacionais e humanas para proteger esse modelo de negócio. Portanto, nós fazemos uma abordagem *top-down*. No topo, definimos muito bem o modelo de negócio e depois começamos a "descer" e a integrar tecnologia. Há uns anos não era bem assim, primeiro reuniam-se as caixas, a tecnologia, e depois é que se pensava no negócio.

Visionware foi recentemente credenciada pelo Gabinete Nacional de Segurança, é aliás a única empresa a deter esta credenciação, e tem ainda as principais Certificações internacionais em Segurança de Informação. Que vantagens isto traz para empresa, nomeadamente ao nível do mercado, e o que mudou em termos de exigência?

Nós já tínhamos um conjunto de credenciais internacionais a nível individual, diria que quase todos os nossos fornecedores têm alguns dos maiores carimbos que há a nível internacional face à concorrência, que também não é muita. Em suma, demos três, quatro passos à frente.

Como surgiu a parceria estratégica com a Edisoft, que detém 50% do capital da Visionware, e que impacto está a ter na actividade da empresa?

A Visionware rapidamente teve um grande impacto no mercado nacional. O primeiro ano foi de investimento e o segundo foi um boom imediato. Tivemos vários "assédios" das maiores empresas nacionais que recusámos, por termos uma capacidade financeira muito interessante. Tivemos o cuidado de dizer que não a todas as propostas porque entendemos que eram uma mera aniquilação do concorrência por aquisição. Já o caso da Edisoft foi completamente diferente.

Primeiro, tínhamos uma relação interessante ao nível de parceria, segundo, porque a Edisoft trabalha num mercado em que queríamos entrar rapidamente, o mercado de Defesa, a um nível NATO e de Defesa interna, a que não tínhamos acesso e onde a Edisoft domina.

A Edisoft tem também um conhecimento muito grande em sistemas de desenvolvimento no sector espacial e do mercado internacional, uma área onde queremos entrar, e além disso tem uma estrutura associada, vinda da Empordef, que também nos interessa. Paralelamente, a Edisoft trabalha em projectos onde a componente de segurança lógica começa a ser um requisito fundamental quando se fala em NATO. Daí a parceria ter sido imediata. Como actuamos em áreas de mercado não concorrentes esta parceria só podia ser benéfica para ambos e gerou-se uma grande amizade.

"CASO ESTÓNIA EM PORTUGAL SERIA CATASTRÓFICO"

O recente caso Estónia – pais que teve de pedir ajuda à NATO – é um exemplo de guerra electrónica e de informação feito pela Rússia, e o primeiro caso que abre uma nova perspectiva da guerra, na senda da teorização dos coronéis chineses de "guerra irrestrita". Se fosse em Portugal, como seria?

Nós tivemos, há pouco de tempo, um conjunto de pessoas israelitas que tiveram a dar formação à Visionware sobre alguns equipamentos que vão agora entrar no mercado. Eles estão muito habituados composente *ciberwar*, porque têm uma área muito forte de Defesa, os índices de protecção são muito elevados.

Lembro-me de um caso, há uns anos, na primeira abordagem na Guerra do Golfo, de um atraso muito grande em termos de ataque aéreo, porque demoraram muito tempo até conseguirem fazer ataques de *ciberwar* para pôr em baixo todos os sistemas de radar. Só depois dos radares em baixo puderam iniciar o ataque aéreo, o que prova uma ligação muito estreita entre a estratégia militar e a *ciberwar*.

Em Portugal... posso confirmar que já existem muitos casos de *ciberwar* junto das maiores empresas e banca e tipicamente tem duas grandes intenções: denegrir a imagem para pôr em causa concorrência, com ataques directos às maiores instituições nacionais, governamentais, banca ou indústria, caso de alterações de homepages com conteúdos maliciosos ou quebra da página do serviço de homebanking de uma entidade bancária, com consequências muito pesadas, em termos de imagem, dado que a segurança e a percepção dessa por parte dos clientes é fundamental; a outra componente que tem vindo a suceder com regularidade são os ataques directos ao negócio, o denominado roubo de informação.

Tivemos vários incidentes em que fomos chamados pelas autoridades, participámos como peritos, e nestes casos fizemos sessões de *forensic*, ou seja, reconstituímos o que aconteceu. Aqui falamos de roubo de informação puro. Vou lhe dar um exemplo, imagine que algumas das nossas maiores individualidades são alvo de um furto de e-mail e depois alguém começa a falar em seu nome com outras pessoas. Isto tem acontecido muito com impactos em termos de imagem.

Estes são os ataques de *ciberwar* mais frequentes. Outro tipo de ataques que sucedem muito são os de *denial of service*, não direccionados, ou seja, afectam todos os que estiverem vulneráveis, com objectivo de destruição pela destruição.

No entanto, um ataque orquestrado em larga escala, em simultâneo, a sites administração pública e empresas, como seria?

Neste momento, se falarmos das principais instituições portuguesas, há um grupo restrito na área da banca com um sistema de defesas perimétricas muito interessante, ao nível das melhores empresas internacionais, mas representam apenas 2%. Se houvesse um ciberataque orientado a uma grande instituição pública eu diria que o impacto seria catastrófico... no mínimo... seria assustador....

ATRASO DE DEZ ANOS

Ainda há muito trabalho a fazer em matéria de segurança?

Muito...mesmo muito... O maior problema já não é a mentalidade, as pessoas sabem que acontece, já lhes aconteceu, por exemplo, todos

ATRASO DE DEZ ANOS

Ainda há muito trabalho a fazer em matéria de segurança?

Muito...mesmo muito... O maior problema já não é a mentalidade, as pessoas sabem que acontece, já lhes aconteceu, por exemplo, todos recebemos spam, um sintoma de que algo na Internet não é saudável. Começam agora os primeiros investimentos, só que temos já um atraso de dez anos, em relação aos países de topo.

Esse poderá ser um sintoma de os decisores terem receio de dizerem que já foram atacados?

Todos os incidentes tratados pela Visionware implicaram um imediato acordo de confidencialidade. É impossível que isso passe cá para fora. Aliás, foi conhecido há uns anos que houve um roubo de dinheiro na área da banca, os maiores bancos nacionais sofreram um ataque grave de phishing, houve roubo de informação e houve uma reposição imediata de dinheiro nas contas dos clientes, o que denota a sensibilidade destas questões.