manchete

Jornal Negócios
Negócios em rede
29-03-2017

Periodicidade: Diário
Classe: Economia/Negócios
Âmbito: Nacional
Tiragem: 18239
Temática: Tecnologia
Dimensão: 1290 cm²
Imagem: S/Cor
Página (s): 2

Segurança

Investimentos em segurança ainda longe do valor seguro

A escalada de ameaças não deixa margem para falhas no campo da segurança, embora a componente física tenha a sua relevância no mercado, o que é certo é que a segurança lógica tem ganho terreno motivada por uma revolução tecnológica que é conhecida como a 4.ª revolução industrial.

De acordo com os últimos dados publicados e que constam no site da Associação Portuguesa de Segurança (APSEI), o sector da segurança privada, incluindo a segurança electrónica, gerava em 2008 cerca de 708 milhões de euros, sendo 550 milhões respeitantes à vigilância humana, 90 milhões à segurança electrónica e 68 milhões ao transporte de valores.

Segundo dados divulgados pela Informa D&B, no final de 2015, dava-se conta de um volume de negócios do sector na ordem dos 710 milhões de euros, mais 1,4% do que em 2014, o que permite de alguma forma identificar um crescimento lento do mercado.

Em 2016, a Informa D&B previa a tendência ascendente das vendas, na ordem dos 2,1%, para esta área da segurança. Ludovico Jara Franco, presidente da Associação dos Directores de Segurança de Portugal, refere que tal como os outros sectores também este tem vindo a sofrer com a crise, estando desde o ano passado em recuperação nas suas várias vertentes.

O volume de riscos e ameaças tem evoluído de tal forma que este será talvez um dos mercados com maior potencial de crescimento nos anos vindouros. Não há como não investir em segurança, embora muitos gestores ainda tentem remediar, mais do que prevenir.

A preocupação com a protecção e a construção de uma estratégia de prevenção nem sempre é uma prioridade para gestores e organizações. Muitas delas só tratam a segurança quando ocorre um incidente ou quando a legislação obriga a que estejam activos determinados parâmetros de segurança física ou lógica.

Embora Portugal não seja um mercado em que a perda desconhecida seja muito expressiva, face a outros países da Europa, o furto externo nos meios comerciais é o principal motivo desta perda, os valores em causa não são alarmantes.

Já no campo da segurança lógica, o crescimento do cibercrime tem despertado muitas mentes para a escalada de ameaças nunca antes pensadas e muitas delas ainda sem resposta por parte das infra-estruturas das empresas.

No Estudo Anual de Segurança 2016 da Cisco, apenas 45% das empresas admitiram confiar na sua estratégia e na infra-estrutura de segurança para detectar e prevenir ataques na rede. Da mesma forma, o relatório Informação de Segurança nas Empresas Portuguesas, desenvolvido no ano passado pela IDC em parceria com a Cisco, mostra que 59% das empresas têm prevista a implementação de uma estratégia de segurança de informação, mas apenas 21% confirmam ter um plano destes já implementado.

710 MILHÕES DE EUROS
foi o volume de negócios em 2015 que o sector da segurança registou em Portugal.

400 MILHÕES DE PESSOAS
são vítimas de cibercrime, em todo o mundo.

78%
dos cibernautas portugueses estão mal informados sobre como se protegerem contra ameaças de cibercrimes.

As empresas portuguesas gastaram em média 12% do seu orçamento de TIC em segurança em 2015, independentemente da sua dimensão. Além do investimento, que ainda não estabilizou no patamar ideal, os especialistas do sector admitem que ainda há muitas estratégias que falham.

O primeiro ponto de fracasso assenta logo na definição do âmbito, ou seja, as organizações e os seus responsáveis devem ter em mente que não é necessário proteger tudo, de tudo. É necessário proteger, e às vezes de forma desproporcional, os activos físicos e digitais que realmente têm valor, mas, para isso, a organização tem de os conhecer, nas suas diversas formas, e encontrar a melhor maneira de os proteger com o menor impacto possível no negócio.

Um outro ponto em que se costuma falhar nas estratégias de segurança é a definição dos indicadores de desempenho (KPI), para se poder entender até que ponto a estratégia está ou não a ter sucesso. Mais uma vez, não se trata de pensar numa óptica de "one size fits all", pelo contrário, tem muito que ver com cada organização e o seu respectivo negócio e a sua exposição ao risco. Mas é importante que estes KPI existam. É frequente as organizações recorrerem a informação externa, nomeadamente associada a certificações.

O estudo revela também que o orçamento insuficiente (62%) e a crescente complexidade dos ataques (47%) são os principais obstáculos para as organizações em termos de implementação de uma estratégia de informação de segurança. Alguns sectores, como o financeiro e Administração Pública, referem também a existência de recursos não qualificados nesta temática como sendo uma questão importante.

Outra área crítica de sucesso refere-se à comunicação, interna e externa, da estratégia de segurança. O patamar de certificação de segurança serve exclusivamente propósitos comerciais, não tendo por trás qualquer compromisso real da empresa para com a segurança.

A verdade é que a segurança de informação não é uma actividade só dos departamentos de TI, destinada a ser testada pelos utilizadores. Aliás muitas empresas a nível mundial colocam a responsabilidade da segurança da informação num Chief Security Officer ou até num Chief Information Security Officer fora dos departamentos de TI. Da mesma forma, a segurança física deve ter uma supervisão e um controlo atento, mantendo-se o acompanhamento permanente de todas as ocorrências e relatórios.

As organizações precisam de encontrar formas de comunicar constantemente a posição de segurança, de modo que as iniciativas internas e externas sejam bem recebidas e tenham o sucesso desejado.

Para todas as empresas, independentemente do país em que desenvolvam a sua operação, do sector ou da sua dimensão, é importante que adoptem uma estratégia de segurança forte e integrada que possa responder a todas as ameaças e que seja baseada em diversos factores como sejam a habilidade tecnológica, a confiança de fornecedores, a formação de todos os colaboradores e a colaboração dentro da indústria.