“Há ainda um longo caminho a percorrer”

securitymagazine.pt/2020/10/05/ha-ainda-um-longo-caminho-a-percorrer

SecurityMagazine 05/10/2020

Bruno Castro, CEO da VisionWare, destaca à Security Magazine que “é crucial trabalhar as pessoas e os processos dentro das organizações, para que a vertente cibersegurança seja incorporada transversalmente”.

Como tem evoluído a percepção do ciber risco por parte das empresas em Portugal?

Infelizmente, ainda existe a ideia de que a aquisição de tecnologiade ponta, como soluções de antivírus, sistemas de firewall ou outras, são suficientes para garantir a segurança. Ao longo dos anos, temos procurado mudar essa mentalidade, procurando explicar que, a par da tecnologia, é crucial trabalhar as pessoas e os processos dentro das organizações, para que a vertente cibersegurança seja incorporada transversalmente, sempre com base nos três pilares que a definem: tecnologia, procedimentos e,cada vez mais, pessoas.

Só assim será possível atingir um nível de maturidade aceitável no que concerne à segurança da informação face às ameaças que vivemos no mundo digital.

No entanto, é também necessário ter em consideração que o tecido empresarial português é muito heterogéneo. Existem empresas extremamente conscientes, que não prescindem de cibersegurança, algumas que a desvalorizam e outras ainda que não têm qualquer percepção do risco. E é, infelizmente, só em virtude de um primeiro incidente de segurança que, muitas vezes, as empresas começam a mudar a forma como encaram a cibersegurança.

Há ainda um longo caminho a percorrer.

Quais são as principais motivações de compra por parte dos clientes ao nível de produtos/soluções de cibersegurança?

As motivações de compra de soluções pelas empresas estão, normalmente, alinhadas com a percepção do risco de cibersegurança que as organizações têm e, muitas vezes, as escolhas e os investimentos feitos assentam no marketing e na capacidade de venda dos fabricantes e não na análise das necessidades.

O foco tem de estar na melhor relação necessidade/qualidade/preço para cada organização, porque, obviamente, as necessidades de segurança de cada organização são especificas dela própria.

Na VisionWare, temos uma visão holística da segurança e, por isso, consideramos que a aquisição de produtos e soluções de cibersegurança é, apenas, uma pequena parte da solução para mitigar o risco. A capacidade de conhecer as nossas próprias vulnerabilidades, através de processos de auditoria,assim como a formação da estrutura humana, desempenham um papel determinante.

É preciso colocar este tema na ordem do dia e alertar o cliente para as várias dimensões da segurança, em que a aquisição de soluções tecnológicas nem sempre é prioritária face a outras vertentes do modelo de segurança a implementar.

Considera que a actual pandemia trouxe impactos à estratégia de gestão de risco das empresas? Que aprendizagens podem retirar empresários e profissionais desta situação?

A actual pandemia teve um impacto tremendo no que respeita o cibercrime e os dados disponíveis comprovam-no. A necessidade de colocar o negócio e a operacionalidade – recursos humanos – disponíveis via internet veio acelerar, de forma brusca, o processo de digitalização de muitas empresas, expondo-as, de repente,ao mundo digital e de uma forma para a qual não estariam ainda preparadas.

As empresas reagiram ao contexto, mas ficaram expostas a novos riscos, sem que tivessem as ferramentas e a capacidade para os gerir. Isto explica o aumento significativo do número de casos de ciberataque detectados.

A pandemia também veio colocar o tema do teletrabalho em cima da mesa. Uma grande maioria das empresas não estava preparada para gerir os ciberriscos que vieram com esta nova realidade.

Felizmente, tivemos empresas que investiram, atempadamente, em cibersegurança e estavam mais preparadas, e outras que procuraram, reactivamente, corrigir a sua estratégia, à medida que passavam por este novo enquadramento social, o que, não sendo o ideal (na óptica da prevenção), é um ponto de partida.

Infelizmente, também nos deparámos com muitos casos em que a falta de investimento e maturidade no tema da cibersegurança, essencialmente por desconhecerem o seu nível de segurança, provocaram graves dissabores e perdas efectivas, com efeitos directos no

negócio.