CISION

Turisver

Tiragem: 6500
País: Portugal
Period.: Ocasional
Âmbito: Viagens e Turismo

Pág: 4
Cores: Cor
Área: 19,50 x 28,50 cm²
Corte: 1 de 1

ID: 69771040 | 01-05-2017 | Equipamentos e Serviços Para a Hote.

>opinião

TEXTO: JOÃO PRONTO*

"Coração que não vê, coração que não sente!" – Uma perspectiva sobre a (In)Segurança da Informação em Turismo

O nosso setor turístico, empresários e profissionais, tem uma certa tendência para ignorar um conceito fundamental em qualquer atividade empresarial que se suporte na informação e no conhecimento para a tomada de decisão: A Proteção e Segurança da Informação e do Conhecimento Organizacional!

Na sociedade contemporânea, em que a tecnologia está omnipresente no setor turístico, no suporte à tomada de decisão dos profissionais de turismo, mas também, possibilitando aos turistas a interação com o serviço turístico, antes, durante e após o consumo turístico, é fundamental projetar, configurar e proteger corretamente a tecnologia, por forma a que todos os intervenientes do setor turístico, confiem e possam tirar proveito da componente tecnológica. Caso contrário, as partes deixarão de confiar na qualidade da informação e conhecimento que lhes é providenciado pelos alicerces tecnológicos, o que trará naturalmente desconfiança e degradação da qualidade do serviço turístico, e consequentemente um decréscimo do consumo turístico…
Permitam-me que partilhe três exemplos paradigmáticos no setor turístico, acerca da criticidade da (in)segurança da informação:

- O proprietário do Restaurante Estorilix, depois de 5 anos de pressão dos clientes, decidiu fornecer-lhes, gratuitamente, acesso à Internet, via wifi, partilhando o código rest_estorilix, que servirá de username e de password. O problema é que o dono do Restaurante decidiu partilhar o acesso à Internet que "alimenta" o acesso dos Pontos de Venda (POS), e, desta forma, sem a implementação de "um sistema de separação de redes" ao nível do equipamento ativo, e/ou ao nível da Firewall, qualquer cliente mais… (não vou adjetivar) consegue aceder aos conteúdos dos POS e eventualmente da rede interna do Restaurante, copiando, alterando ou inclusivamente apagando a informação diária do Restaurante, que é reportada religiosa e mensalmente à Autoridade tributária.

- A Companhia Aérea Estorilix optou por adicionar a funcionalidade de venda de bilhetes online, através da aquisição de uma gateway de pagamentos no sítio estorilixtravel.com e na APP recentemente disponibilizada para os smart phones e tablets. Neste âmbito, os passageiros podiam, inicialmente, adquirir bilhetes até 4 horas antes da hora de embarque dos voos operados pela Estorilix. Acontece que proliferam casos de clonagem de cartões de crédito, que demoram mais do que um par de horas a detetar, e quando o parceiro de transações eletrónicas alertou a Companhia Aérea de que os cartões tinham sido furtados, já os passageiros tinham saído do avião no aeroporto de chegada… A quantidade de transações fraudulentas foi tão expressiva logo no primeiro mês que o parceiro de transações eletrónicas cancelou unilateralmente o serviço, deixando a companhia aérea de vender online os seus bilhetes, gerando crescentes reclamações dos clientes, também nas redes sociais, devido a este recuo nas vendas online. A Companhia Aérea renegociou com o parceiro de transações eletrónicas, agora paga uma taxa superior, e apenas permite a aquisição de bilhetes online, com um mínimo de 24h de antecedência…

- Um rececionista do Hotel Estorilix, acedeu ao pedido de um hóspede em colocar a pen no computador da receção, para lhe imprimir o cartão de embarque, o problema é que a pen estava infetada com Ransomware, e minutos depois todos os computadores do Hotel, servidores de PMS e F&B incluídos, estavam encriptados, sem que o Hotel conseguisse fazer checkins, checkouts, consultas de histórico, emissão de faturas, nem validar chegadas… pois todos os computadores e servidores estavam bloqueados e encriptados. Ironicamente o Hóspede não sabia que a pen estava infetada, e o rececionista esqueceu-se que o procedimento correto era acompanhar o hóspede ao business corner, para que lá imprimisse o cartão de embarque, que foi efetivamente impresso na impressora da receção…

Com estes três exemplos pretendo ilustrar, com exemplos reais, (nesses casos só a Empresa Estorilix é ficção) a importância de se planificar, configurar e manter uma política de segurança da informação, por forma a que as nossas empresas turísticas não fiquem expostas a incidentes tecnológicos que acarretam quantias avultadas de prejuízos…
Note-se que até ao momento evitei, propositadamente, utilizar a expressão "segurança informática", tendo recorrido à expressão "segurança da informação", pois a informática é isto mesmo, um mecanismo automático de processamento de informação e de conhecimento. É um erro admitir que a segurança informática é uma questão exclusiva dos parceiros informáticos e dos filmes de ficção científica. É fundamentalmente uma questão de sobrevivência empresarial.
Há empresas de Rating de Segurança Informática que classificam e alertam, com base em diversos parâmetros, o potencial de intrusão tecnológica. No nosso setor turístico já existem diversas empresas e instituições que são adeptas e clientes deste tipo de serviços de informação. É vital, para as organizações, ter noção da potencial exposição ao risco tecnológico, bem como à exposição dos parceiros de negócio, com quem se troca enormes quantidades de informação diária…
Nos dias que correm, os conceitos como Anti-Vírus, Backups, Política de Acessos Informáticos, Firewall, httpS, Virtual Local Area Network, …são conceitos que os atuais players das Empresas e das Instituições Turísticas Nacionais e Internacionais têm que levar em (elevada) consideração…
Quanto custará a um restaurante ficar sem a possibilidade de gerir pedidos de mesa, de emitir faturas e perder irremediavelmente faturas e notas de crédito? E numa Companhia Aérea, qual o real prejuízo financeiro se o fornecedor de pagamentos eletrónicos barrar as vendas online durante 24h? E para um Hotel independente, qual o prejuízo de ficar 24 a 72h sem conseguir reconhecer as reservas, emitir faturas, efetuar checkins e checkouts?
Não vou questionar as questões legais inerentes ao acesso à Internet de um cliente num restaurante ou num Hotel, a sites pouco recomendáveis, originando a visita das forças policiais, solicitando informação acerca do acesso em questão… Também não irei questionar as repercussões políticas e económicas da perda de confiança dos turistas, em adquirir produtos e serviços turísticos com receio que os seus dados pessoais, entre os quais os financeiros, passem para mãos erradas….
Não podemos mais olhar para estas questões de (in)Segurança Informática como algo que não é real… coração que não vê… neste contexto, é um coração que sente, e muito!

***João Pronto**
Professor Adjunto da Escola Superior de Hotelaria e Turismo do Estoril
Professor Convidado da Católica Porto Business School
Consultor de IT em Empresas Turísticas

Nota: O autor escreve ao abrigo do novo Acordo Ortográfico