Turisver

“(in)Segurança Tecnológica em Hotelaria e Turismo”, por João Pronto

13 Junho 2023 Opinião

Num mundo em que os ataques informáticos estão cada vez mais presentes, seja no dia-a-dia das pessoas como das organizações, a temática da (IN)Segurança tecnológica em Hotelaria e em Turismo ganha importância acrescida e é sobre este tema que João Pronto fala neste artigo.

João Pronto, ESHTE

Professor Especialista em Hotelaria e Restauração

Professor Adjunto – Ciências da Informação e Informática

Coordenador de Estágios

Há três temáticas às quais dedico mais tempo de estudo, reflexão e implementação, quer como cidadão, professor ou informático/eletrotécnico:

A) Otimização de Processos de Negócio (com principal enfoque na hiper-personalização da experiência Hoteleira e Turística) – temática que recorrentemente escrevo artigos de opinião, e que se tem revelado como uma fonte inesgotável de conhecimento.

B) Inteligência Artificial (foi claramente a temática que mais me apaixonou aquando da minha já longínqua licenciatura, ao ponto de mais tarde *a* ter escolhido como base de fundamentação da dissertação de Mestrado no IST "Turistólogo, o Ciberturista – Um Sistema Pericial"), e não mais tirei da cabeça esta apaixonante e desafiante temática, que hoje em dia, como sabemos, está-nos a desafiar *à séria* com a abordagem do ChatGPT, e razão pela qual escrevi os dois últimos artigos de opinião, aqui na Turisver.

C) (in)Segurança dos sistemas de informação em geral, e das organizações hoteleiras e turísticas em particular, é uma temática que persiste nos meus estudos e nas minhas preocupações diárias de utilizador de sistemas de informação, como forma de aceder e partilhar conhecimento, com os meus amigos, família, alunos e colegas de trabalho.

É sobre a temática da (IN)Segurança tecnológica em Hotelaria e em Turismo que me vou debruçar neste artigo, e no qual, vou ter de *pesar* e refletir muito bem as palavras que escrevo, dada a criticidade e atualidade extrema do tema.

Como é sobejamente sabido e debatido, o Turismo em geral e a Hotelaria em particular, vivem da qualidade do serviço prestado e da segurança com que prestam o serviço turístico.

No entanto, temos sempre de ter bem presente que o serviço turístico é:

Fortemente suportado por tecnologia ao nível dos processos internos das organizações turísticas;

Progressivamente requerido por turistas e por hóspedes, que o serviço turístico seja prestado diretamente aos próprios via tecnologia, e de forma explícita;

A relação das organizações turísticas com fornecedores e parceiros de negócio é muitíssimo mais suportada por tecnologia do que era há um par de anos atrás, o *confinamento* que tivemos com a pandemia do Covid19 agilizou de forma muito expressiva a

massificação da tecnologia em geral e das relações via Internet em particular, sem que a sociedade tivesse tempo de se ajustar.

Os ataques informáticos estão progressivamente mais presentes no nosso quotidiano pessoal e profissional, e a esmagadora maioria das pessoas persiste, erradamente, em negligenciar práticas e processos pouco cuidados de interação com a tecnologia, onde a famosa expressão portuguesa tem um impacte brutal na nossa vida "coração que não vê, coração que não sente". No final deste artigo irei dar exemplos práticos deste nosso triste e-fado.

Retomemos os processos internos das organizações turísticas e hoteleiras, explanando-os mais concretamente:

Os processos internos das organizações estão muito mais suportados e dependentes da tecnologia do que alguma vez aconteceu.

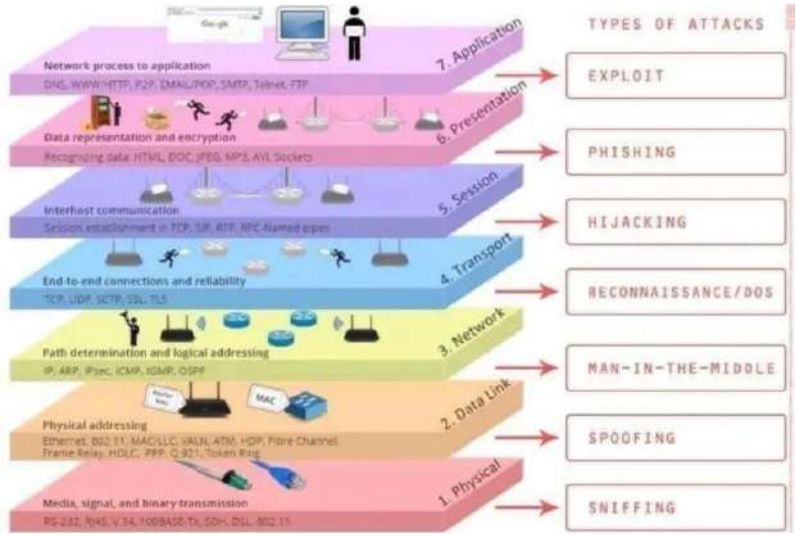
A esmagadora maioria das organizações turísticas disponibiliza aos seus colaboradores, (não só aos que trabalham em *back-of-the-house* como aos que trabalham diretamente com os turistas) um computador fixo ou portátil e um telemóvel, em que os colaboradores partilham, através destas duas tipologias de dispositivos, não só o seu conhecimento organizacional, mas também o conhecimento e os dados organizacionais do departamento ao qual pertence, e, cumulativamente, os dados de outros departamentos da organização aos quais tem acesso. Há inclusivamente organizações, também turísticas e hoteleiras, em que quase todos os colaboradores acedem a quase todo o conhecimento organizacional, com todas as vantagens e desafios inerentes a esta abordagem de partilha de conhecimento.

Há também, infelizmente, muitas organizações que durante a pandemia, e não mais "emendaram a mão", solicitaram aos seus colaboradores para utilizarem o computador pessoal ou o telemóvel pessoal, para acederem aos sistemas de informação da organização, com principal enfoque no email e nas aplicações *coore* da empresa, através da implementação de uma VPN no computador pessoal, ou pior, através de um endereço público, sem qualquer proteção de certificado digital e de encriptação forte.

Principal "calcanhar de Aquiles" desta abordagem, vou denominar de "caseira", para não ser antipático para com as pessoas e organizações que utilizam este tipo de abordagem, é obviamente a falta de segurança da informação partilhada nas organizações com este tipo de abordagem, porque os computadores pessoais não têm, muitos deles, nem anti-vírus (nem que seja grátis), nem são geridos pelo anti-vírus corporativo, ou pelo servidor que gere os utilizadores organizacionais e muito menos pela Firewall organizacional (quando existe).

Para piorar, estes e outros utilizadores partilham o email organizacional para aceder às redes sociais e para configurar aplicações pessoais, muitas delas com graves falhas de segurança, provocando inúmeras potenciais portas de entrada.

Não me vou alongar acerca do famoso modelo OSI (Open System Interconnection) que define a arquitetura de comunicação em rede, através da interconexão de 7 camadas… pensemos só um segundo sobre o assunto: cada uma das camadas têm pelo menos um tipo de potencial ataque informático…



(Cisco)

A partilha de fotografias e de vídeos é normal nos dias de hoje, o problema é que há fotografias e vídeos que têm links associados, em que nós, ao clicarmos nos mesmos, somos direcionados para sites que se "limitam a recolher o pedido de acesso efetuado a partir do nosso computador ou telemóvel" e a partir desse momento, o atacante tem acesso direto ao que se passa no nosso computador, sem que nós tenhamos a mais pequena ideia do que realmente se está a passar.

Então, se assim é, antes de clicarmos numa fotografia ou vídeo, devemos antes de clicar, verificar se o cursor de seleção muda formato, indicando-nos que se trata apenas de uma fotografia ou de um vídeo, ou se, pelo contrário, tem um link atribuído que nos leva para um site onde um atacante espera *ser convidado* a aceder ao nosso equipamento informático…

Por esta e por outras razões é que se estão a massificar os acessos empresariais com a tecnologia .IX, a implementação de dupla autenticação forte via APP instalada no telemovel, e ainda a utilização obrigatória de ferramentas de MDM (Mobile Device Management) que tem como principal propósito implementar uma política de "bolha" nos nossos dispositivos de trabalho e/ou lazer protegendo-nos de ataques externos e/ou internos.

Aconselho vivamente a que cada um de nós, dedique progressivamente um pouco mais de tempo e de atenção a esta temática, estando mais alertas para a informação que acedemos e partilhamos online, por forma a não clicarmos em todas as fotos e vídeos que nos enviam, mesmo que tenham sido enviadas, supostamente, de quem confiamos e muito, evitando que o nosso ambiente de trabalho se transforme na imagem abaixo apresentada, (fonte, El Mundo), impedindo o acesso aos ficheiros existentes no computador em questão, ou, pior, impedindo o acesso a todos os servidores e computadores da rede interna, que estavam ativos aquando do ataque.

Infra, podemos verificar alguns ataques em tempo real detetados pela *Checkpoint* (um dos principais fornecedores de ferramentas de *Firewall*), https://threatmap.checkpoint.com/

Para terminar este artigo, deixo algumas recomendações de boas práticas na utilização de tecnologia, no nosso quotidiano de trabalho/lazer:

Todos os computadores, sem exceção, devem ter o sistema operativo (Windows, Linux, OS X) atualizado, com antivírus também atualizado.

É imperativo que toda e qualquer empresa/instituição turística tenha uma ou mais *Firewall* de última geração, para que consigam intercetar códigos maliciosos em *email* e na *web, bem como gerir os acessos internos e externos à organização*.

Estas *Firewall*, devem, para além de barrar determinado tipo de acessos do exterior, cumulativamente, têm o poder de monitorizar e informar quem de direito, sempre que sejam detetados determinados tipos e/ou tentativas de acessos indesejados.

É também imperiosa a existência de uma política concreta de acesso à informação interna, e à informação proveniente de clientes, fornecedores e parceiros de negócio. A implementação de políticas de *password* e de controlo de acessos informáticos, é fundamental e obrigatória!

A tradicional abordagem "coração que não vê, coração que não sente", do ponto de vista tecnológico, já não faz qualquer sentido, e ainda aí vem mais legislação concreta que "obrigue" os *players* turísticos e proteger condignamente os dados pessoais dos seus clientes… é portanto, fundamental, termos todos noção de que os nossos sistemas informáticos são compostos por diferentes níveis de acesso, como se tratassem de peças de Lego, em que temos de proteger todas estas ligações, porque, demasiadas vezes, os ataques informáticos não são sequer detetáveis na interface gráfica à qual o utilizador tradicional acede… como acima verificámos com os pelo menos 7 tipologias de ataque acima referenciados no Modelo OSI.

Temos então, que proteger todas estas camadas que se interligam, e que, no seu todo constituem o nosso sistema de informação/conhecimento da nossa organização, seja empresarial ou institucional.

Como venho afirmado, demasiadas vezes para o meu gosto, vamos todos ser atacados, algum dia, com sucesso (do ponto de vista do atacante, claro está), o que devemos então de fazer? Prepararmo-nos para que esse dia chegue o mais tarde possível, não facilitando e estando alerta também *online*, e quando chegar o momento, que temos procedimentos tão ágeis quanto possíveis, de reposição do sistema informático que suporta toda a nossa informação organizacional.

Tendo noção de que a esmagadora maioria das nossas organizações turísticas são de muito pequena dimensão, em que o conceito "Segurança Informática" é algo de abstrato e difuso, creio que este será um tema crescentemente recorrente, nos próximos meses e anos…

A 23 de maio passado, estive num evento Host Level-Up, organizado pela HHS, que teve a amabilidade de me convidar para mediar um painel de debate – Cibersegurança 360^0: Proteja o seu Hotel, nos quais Rui Alves, Diretor de Tecnologias de Informação dos Hotéis Porto Bay, e Pedro Moita, Pro-Presidente da ESHTE debateram e alertaram quem estava presente, as boas práticas de implementação de segurança informática Hoteleira.

Foi absolutamente esclarecedor a quantidade de experiências e partilha de conhecimento que pudemos assistir, a frequência de experiências semelhantes subordinadas a esta temática, é absolutamente imperioso, dada a criticidade da temática.

Em jeito de conclusão, é sempre possível *baixar o nível*: há relatos de que as grandes multinacionais de reservas turísticas também estão vulneráveis e alegadamente sucedem, de forma crescente, casos de reservas turísticas fictícias… o manancial de escrita de artigos relativos a esta temática é quase tão promissor quanto o arrepio na espinha que sinto quando escrevo este tipo de artigos…

Quero com este artigo alertar, muito claramente, a duas situações complementares:

1. Temos de proteger os nossos sistemas informáticos de forma efetiva, adquirindo as ferramentas necessárias para que seja mais difícil aos atacantes, entrarem nos nossos sistemas informáticos;
2. Devemos manter um comportamento responsável na utilização quotidiana do nosso sistema informático, pois de muito pouco servem as ferramentas de proteção informática, se mantivermos uma postura irresponsável e muito pouco cuidada, provocando o colapso da nossa informação e das pessoas que connosco trabalham.

De que me servem airbags e todo o sistema de segurança implementado no mais seguro dos carros, se eu displicentemente e de forma consciente conduzo a 200Kmh contra um muro de betão?

Nos sistemas de informação também devemos de ter a consciência do que devemos ou não devemos clicar ou partilhar… para bem da nossa e-saúde, e das nossas organizações.

← ARTIGO ANTERIOR
Primeira loja conjunta DS Imobiliária e DS Travel inaugurada em Sines

PRÓXIMO ARTIGO
"Quem Avisa Amigo É", por Atilio Forte

Artigos Relacionados

Turismo Centro de Portugal promove-se em duas feiras em Espanha

21 Setembro 2022 Destinos

Deixe uma resposta

O seu endereço de email não será publicado. Campos obrigatórios marcados com *

Comment *

Name *

Email *

Website

Guardar o meu nome, email e site neste navegador para a próxima vez que eu comentar.

Publicar comentário

Pesquisar

Opinião

“(in)Segurança Tecnológica em Hotelaria e Turismo”, por João Pronto

Ler Artigo »

João Pronto, ESHTE
Professor Especialista em Hotelaria e Restauração
Professor Adjunto – Ciências da Informação e Informática
Coordenador de Estágios

“Glória aos vencedores!”, por Miguel Paredes Alves

Ler Artigo »

Miguel Paredes Alves
CEO, HotelShop

“Não Há Pior Surdo…, Nem Pior Cego…”, por Atilio Forte

Rumores

Nesta Rubrica, o Turisver.pt dá-lhe conta do que se vai dizendo e passando nos “corredores” do Turismo.

Clique aqui »

Últimas Notícias

Área de corporate da BCD vai integrar o Grupo Ávoris em Portugal

Pedro Gordon: Entrada do Grupo Newtour "marca uma nova etapa" na vida da GEA

Carlos Moedas exige eletrificação do terminal de cruzeiros e pagamento da taxa turística

Fundação INATEL adere à Airmet para reforçar afirmação no mercado

Nortravel inicia operação charter para a Boa Vista

Melhores empresas do mundo buscam alunos na Les Roches Marbella

Cruise Division do MSC Group divulga plano de energia em terra 2024-2026

Promoções

- Cruzeiros
- Operadores

Pontos nos Is

"Acredito que, para se ter sucesso, não se pode arriscar no escuro. Tenho sempre este princípio para os negócios e até para a vida". "Nada me dá mais prazer do que chegar a um sítio, imaginar algo para lá e depois ver essa ideia concretizar-se".

Jorge Rebelo de Almeida, Presidente do Grupo Vila Galé
In: Expresso, 2 de junho de 2023

"Este está a ser um bom 2023, o movimento nos aeroportos cresceu 13% em janeiro, 19% em fevereiro e 14% em março. Em abril ainda não sabemos, mas já sabemos que temos a Páscoa completamente cheia, vai ser um bom ano. Costumo dizer que 2022 foi o ano do sorriso para o turismo e 2023 continua a confirmar o que aconteceu no ano passado".

Francisco Calheiros, Presidente da Confederação do Turismo de Portugal
In: TSF, 8 de abril de 2023

Turisver

A informação de turismo indispensável aos profissionais.

Links Úteis

Contactos

Estatuto Editorial

Política de Privacidade

Siga-nos nas Redes Sociais

Newsletter