Cibersegurança em hotelaria: uma resposta reativa ou proativa?

Para aproveitar os benefícios do digital, é necessário planear uma estratégia de cibersegurança que permita mitigar os riscos possam surgir. Estarão os hoteleiros preparados para um potencial ataque cibernético?

Texto **Carla Nunes** Fotografia **DR**

O ÚLTIMO RELATÓRIO de riscos e conflitos do Centro Nacional de Cibersegurança Portugal (CNCS), publicado em junho de 2022 com dados referentes a 2021, dava conta de que a percentagem de crimes relacionados com a informática em relação ao total de crimes registados em Portugal cresceu 0,4 pontos percentuais, de 7,4% em 2020 para 7,8% em 2021.

No mesmo documento é apontado que "os setores mais afetados pelos incidentes de cibersegurança são a Banca, as Infraestruturas Digitais e os Prestadores de Serviços de Internet", sendo que "a área governativa com mais incidentes registados é a Presidência do Conselho de Ministros", de acordo com dados registados pelo CERT.PT, uma equipa de resposta a incidentes de segurança informática nacional que integra o CNCS.

Neste contexto, como podem os hoteleiros

proteger as suas operações? A Publituris Hotelaria reuniu um conjunto de especialistas para responder à questão e simplificar o conceito de cibersegurança.

Quando falamos de cibersegurança referimo-nos a "uma área de atuação e processo tecnológico contínuo que visa proteger e manter em segurança toda a informação digital e infraestrutura tecnológica de uma organização", tal como explica Fernando Amaral, CEO da Alidata.

No entanto, o profissional faz a ressalva: "Digo 'visa proteger', pois a segurança a 100% nunca pode ser garantida. Trata-se de um processo contínuo de investimento em atualização tecnológica e formação das pessoas. Não basta instalar um conjunto de ferramentas. É fundamental a sua atualização permanente, formação dos colaboradores e implementar um conjunto de processos e boas práticas".

Sobre este assunto, Pedro Veiga, consultor em cibersegurança e ex-coordenador do Centro Nacional de Cibersegurança, acrescenta que "a gestão de topo de uma organização deve ter a perceção de que a presença no mundo digital atual tem de ser acompanhada de investimentos em meios técnicos e humanos, bem como adaptações organizacionais, para poder aproveitar os benefícios do digital – em paralelo com a mitigação dos riscos possam surgir".

Quais são os riscos?

Quando questionados sobre as ameaças mais recorrentes, todos os entrevistados são consensuais: o ***phishing*** e ***smishing*** – conhecido como o roubo de *passwords* e que pode ser realizado via email ou mensagens de texto – e o ***ransomware***, no qual o *hacker* controla os dados de uma organização e exige um resgate (*ransom*) para desbloquear o sistema.

"O histórico dos ataques a este setor [da hotelaria] indica que a maioria visa o roubo de dados do negócio – bases de dados de clientes e com informação de meios de pagamento – ou bloqueio das infraestruturas digitais que impedem o normal funcionamento, com recurso a *ransomware*, e o correspondente pedido de resgate. Sistemas impedidos de funcionar durante horas representam prejuízos, daí os pedidos de resgate para desbloquear os sistemas", explica Pedro Veiga.

Outra das ferramentas utilizadas no cibercrime é o ***malware***, que consiste no uso de *software* para prejudicar um sistema – os conhecidos vírus, *spywares*, *worms*, cavalos de Tróia, entre outros, como apontado por Fernando Amaral.

No entanto, e "devido à proliferação de dados de cartões crédito e dados pessoais, existem riscos de cibercrime específicos à hotelaria, como por exemplo, os ataques orientados aos sistemas de POS", aponta Marco Correia, CIO na Mercan Properties.

Este profissional é da opinião de que "a mentalidade de orientação para o serviço e de querer facilitar os pedidos de clientes faz com que existam inúmeros relatos de entidades turísticas que foram sequestradas ou tiveram perdas muito significativas de dados através de **engenharia social**" – uma outra ameaça apontada por Fernando Amaral e que consiste em explorar erros humanos para obter acesso a informações ou serviços.

"Geralmente, a engenharia social faz com que as vítimas abram ficheiros ou e-mails, visitem websites e, assim, concedam acesso não autorizado a sistemas ou serviços. O ataque mais comum deste tipo é *phishing*, por e-mail, ou *smishing*, por meio de mensagens de texto", explica o CEO da Alidadta.

Por essa razão, todos os especialistas entrevistados são unânimes ao afirmar que a formação dos funcionários da organização "é crucial".

Para Paulo F. Cardoso, especialista em segurança de informação na PFC Consulting, "a formação dos colaboradores nas vertentes da engenharia social é o primeiro passo [para uma estratégia de cibersegurança]. Ensinar às pessoas as formas mais comuns de como podem ser enganadas e de como evitá-lo diminuiria drasticamente o número de ataques que terminam com sucesso", defende.

Também Pedro Veiga é da opinião de que "há que capacitar os recursos humanos a todos os níveis para estarem atentos aos cibercrimes tradicionais, mas também aos novos desafios que surgem", com "formação frequente de todo o pessoal, em particular aos cibercrimes que se dirigem a explorar a ingenuidade das pessoas como porta de entrada na infraestrutura digital da organização".

Em suma, Fernando Amaral defende que "a atualização e investimento contínuo em tecnologia, bem como a formação de colaboradores, devem fazer parte da política estratégica da organização de forma proativa, e não apenas reativa".

Quem está em risco?

Tanto para Marco Correia como para Fernando Amaral, a mentalidade de que "uma empresa pequena não é apetecível para um cibercriminoso não é correta" – até porque, tal como o CIO da Mercan Properties explica, "muitas das tecnologias de *malware* são auto-

FERNANDO AMARAL, CEO da Alidata

MARCO CORREIA, CIO na Mercan Properties

>>>

>>>

matizadas e literalmente varrem a internet em busca de sistemas vulneráveis".

Sabendo que "os cibercriminosos atuam para obter ganhos financeiros", estes dirigem-se "preferencialmente a grandes empresas, onde os ganhos resultantes possam ser maiores", como apontado por Pedro Veiga. No entanto, é importante lembrar que "todos estão em risco".

"Não se trata de indicar se a empresa vai ser atacada, mas quando. Somente os impactos serão diferentes. Numa grande empresa haverá um impacto mediático e reputacional significativo. [No entanto], é recorrente os atacantes recorrerem a empresas mais pequenas – tipicamente fornecedores das empresas maiores – para prepararem o ataque à empresa cliente. As vulnerabilidades tendem a ser em maior número e os controlos menos apertados que na empresa cliente, e isso é aproveitado", explica Paulo F. Cardoso.

O consultor Pedro Veiga lembra que "todas as empresas devem investir recursos adequados para se protegerem", dando o exemplo do caso hoteleiro, que fornece acesso wi-fi aos clientes. "Muitas vezes os equipamentos usados e os mecanismos de autorização são débeis. Compram-se *routers* Wi-Fi "baratinhos" e afixam-se as *passwords* de acesso publicamente. Devem ser instalados equipamentos com níveis de segurança elevada e que serão mais onerosos, já que os *hackers* têm facilidade em identificar a marca e modelo dos *routers* – se forem de determinados tipos, são fáceis de penetrar, expondo a rede da organização", explica Pedro Veiga.

O profissional acrescenta ainda que "as redes da empresa, dos funcionários e dos clientes também devem estar devidamente separadas, e os bens digitais mais críticos, como dados, serviços, aplicações, com acesso muito controlado".

"Dá trabalho, mas tem retorno em termos de cibersegurança", garante.

– **PAULO F. CARDOSO,** especialista em segurança de informação na PFC Consulting

– **PEDRO VEIGA,** consultor em cibersegurança e ex-coordenador do Centro Nacional de Cibersegurança

O que podem os hoteleiros fazer para se protegerem?

Paulo F. Cardoso é taxativo ao afirmar que "o facto de não existirem recursos não é desculpa para não se implementarem controlos básicos" – até porque "o Centro Nacional de Cibersegurança dispõe de formação gratuita e de qualidade".

Também o CEO da Alidata afirma que "as boas práticas micro estão ao alcance de qualquer pequeno hotel independente e têm a mesma validade para um grupo hoteleiro multinacional".

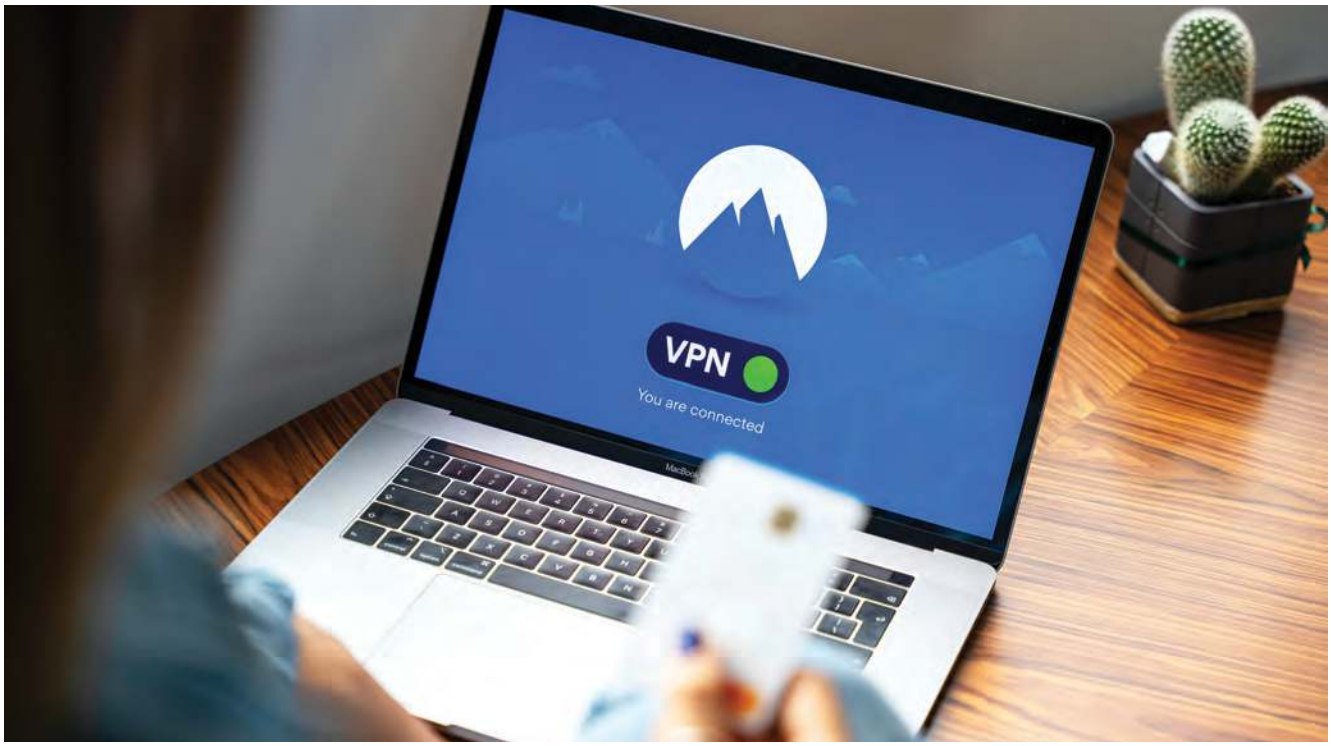
Por essa razão, elencamos abaixo algumas medidas básicas de cibersegurança apontadas pelos quatro entrevistados:

- Proteção das infraestruturas digitais (como redes, servidores, equipamentos terminais, serviços e aplicações), com ênfase nos sistemas de autorização e autenticação;
- Criação de cópias de segurança frequentes, atualizadas e redundantes, que devem ser guardadas fora do espaço físico da organização e *offline*;
- Ter postos de trabalho, em especial os que sejam móveis e possam ser roubados ou perdidos (como portáteis, *tablets*, *smartphones*), com segurança reforçada – seja com controlo por *smart card* ou biometria (com impressão digital, por exemplo);
- Palavras-passe seguras e exclusivas;
- Ativação de fatores de dupla autenticação sempre que possível – ou seja, não utilizar apenas *username* e *password*, mas também um código aleatório em cada acesso. Se possível, evitar o uso do SMS, que é mais vulnerável;
- Manter um *software antimalware* ativo e atualizado, preferencialmente que sirva também de *firewall*;
- Atualizar com as versões mais recentes o *software* existente – sistema operativo e aplicações;
- VPN;
- Redes de wi-fi seguras e acesso remoto seguro;
- Não abrir ligações e anexos suspeitos.

À listagem, Pedro Veiga aponta para a necessidade de "ter políticas de uso dos recursos restritivas que, não sendo fáceis de impor, são fundamentais para reduzir o risco". Dá como exemplo a proibição de uso de *pen-drives*, "que podem ser uma porta digital escancarada ao roubo de dados ou à entrada de *malware* (*software* malicioso)". Como alerta, "muitos problemas são internos, desde um funcionário descuidado, descontente ou sem princípios éticos e que prejudica a empresa onde trabalha".

Existindo disponibilidade financeira para investir em cibersegurança, "e sendo o risco significativo, incluindo o reputacional", Paulo F. Cardoso defende que se "deve contratar um especialista para analisar a situação concreta da empresa", uma opinião coincidente com a de Marco Correia, que também aponta para a contratação de "serviços de cibersegurança geridos por um fornecedor especializado".

>>>



>>> "A temática da cibersegurança é de elevada complexidade e é extremamente difícil para organizações de pequena e média dimensão, como são a maioria das empresas hoteleiras nacionais, adquirir e reter as competências necessárias dentro de portas", afirma o CIO da Mercan Properties.

Em jeito de provocação, Fernando Amaral afirma que "a pergunta que os empresários devem fazer é: quanto custa ser atacado?

O panorama da cibersegurança em Portugal

Quando questionados se as preocupações com a cibersegurança estão bem cimentadas em Portugal, todos os entrevistados dão conta de que "ainda há caminho a percorrer" nesta área.

Para Pedro Veiga, existe no país "uma cultura de segurança 'flexível', que nos leva a julgar que 'isso só acontece aos outros' e que 'somos bons no desenrasca', por isso, planeamos de modo insuficiente". No entanto, o profissional lembra que "o mundo digital, o ciberespaço, penetrou de modo permanente no nosso quotidiano", obrigando a "uma abordagem diferente, mais exigente", sob pena de não "aproveitarmos os benefícios da digitalização da sociedade na sua plenitude".

Já Paulo F. Cardoso é da opinião de que "estamos muito longe do que considero razoável", sendo para isso necessário um investimento na educação para a segurança da informação, "que deverá começar nas escolas e ser implementada nas empresas".

"Tem de ser tão comum mudarmos a *password* de acesso aos nossos *routers* em casa após a instalação como colocar o carro na garagem para que não seja roubado" refere o especialista da PFC Consulting.

Este aponta ainda para "o enorme défice de especialistas para ajudar nesta tarefa", estimando que, "no mundo, rondam os seis milhões, de acordo com alguns estudos": "Um especialista demora anos a formar, [pelo que devem] validar-se as suas certificações antes da contratação".

No entanto, há alguns cenários otimistas. Para Marco Correia, apesar de o "nível da literacia digital das empresas ser média a baixa", no que diz respeito à hotelaria "o esforço de modernização em sistemas críticos, como por exemplo o PMS ou o processamento de cartões de crédito, é notório" – embora "ainda exista caminho a percorrer".

Já Fernando Amaral garante que "a Covid fez mais pela cibersegurança e transformação digital que os nossos consultores nos cinco anos anteriores – eu incluído". De acordo com o profissional, "a pandemia veio colocar o tema na agenda, tal como os ciberataques a reputadas empresas que operam em Portugal também reforçaram".

"Como se diz nesta área, e sobre ciberataques, há três tipos de empresas: as que já foram atacadas, as que vão ser e as que ainda não sabem que foram", termina. **h**