Os mais recentes ataques informáticos a várias entidades levantam a questão: qual o nível de segurança informática que existe no setor do turismo em Portugal?

João Pronto, professor Adjunto, Internship Coordinator da ESHTE

(In)Segurança Informática no Turismo

O nosso tecido empresarial e público em geral, o Parlamento, o Grupo Impresa, a Vodafone Portugal, e outros players menos mediáticos, têm sido atacados (infelizmente) com sucesso, colocando a nu o desgraçadamente famoso "calcanhar de Aquiles" tecnológico. A INsegurança crónica dos processos de utilização e gestão dos diferentes níveis da afamada camada OSI dos Sistemas de Informação.

Mas o que é a camada OSI - Open Systems Interconnection? Pergunta o leitor menos versado nas componentes mais técnicas da tecnologia.
A resposta é direta, terrivelmente simples e complexa: é uma com-

ponente conceptual que permite identificar e desenvolver os diferentes níveis que compõem os diversos subsistemas informáticos, fornecendo-lhes o que todos nós utilizadores ambicionamos: a capacidade de diferentes equipamentos tecnológicos de comunicarem uns com os outros, independentemente de serem mais ou menos evoluídos, sem que os utilizadores (que podem ser ou criadores de conteúdos, ou apenas consultores de conteúdos) se preocupem minimamente qual o equipamento que devem utilizar para aceder a determinado conteúdo ou a determinada tecnologia.

No entanto, esta portabilidade incrementa exponencialmente a probabilidade de deteção de vulnerabilidades entre as camadas e, obviamente, dentro das próprias camadas OSI e porque é que estou a escrever estas linhas mais técnicas quando a esmagadora maioria das pessoas que leem estes meus artigos são profissionais turísticos?

Porque é através destes diferentes níveis que os atacantes acedem aos sistemas, sem que os profissionais das organizações turísticas deem por isso, mesmo quando estão a utilizar o próprio computador.

E as empresas e organismos turísticos? Como têm passado e o que vão passar nos próximos tempos, com este incremento significativo de ataques informáticos?

Permitam-me enquadrar o tema.

Algures no final de maio de 2017, escrevi um artigo numa outra publicação turística, sobre esta temática da Segurança Informática, dado que na altura tinha ocorrido um ataque informático sem precedentes, à escala europeia e nacional, com enorme impacte em diversas multinacionais de tecnologia, que providenciam serviços informáticos a inúmeras empresas e instituições turísticas, designadamente serviços de email e serviços de cloud, como backups online, áreas de trabalho na cloud, acessos internet, entre outros.

O maior constrangimento tratou-se ao nível da gestão de email, pois o ataque foi direcionado por esta via, em que os atacantes enviaram massivamente email para caixas de correio empresariais, e, quando pelo menos um dos colaboradores de determinada instituição/empresa turística/de tecnologia abriu o email e carregou num link ou num ficheiro anexo ao email, contendo código malicioso, o malware (MALicious SoftWARE) propagou-se automaticamente por toda a rede interna da instituição/empresa turística/ tecnológica em questão encriptou grande parte ou todo o sistema informático da instituição/empresa atacada.

Consequências? Quem abriu e ativou inadvertidamente estes conteúdos de email e não desligou a tempo todos os servidores e computadores internos, ficou literalmente sem sistema informático.

O ambiente de trabalho transformou-se 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.

Continuo, quase numa abordagem religiosa, a aceder e a analisar a evolução destes ataques, à escala global, e comparei o resultado o écran de ataques detetados pela Checkpoint (um dos principais fornecedores de ferramentas de Firewall), onde também é possível observar que, à escala global, o número de ataques detetados por esta plataforma, disparou de uns assombrosos (maio de 2017) 3,617,008 ataques detetados para (10 de fevereiro de 2022) 42,744,788 ataques detetados!!!!

Lamentavelmente, teremos que admitir que, nos casos da INsegurança informática, a probabilidade de "nos bater à porta o infortúnio" é elevada, mas não temos que lhes facilitar a vida!

Assim, reitero 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.

Nas organizações deverão ser os servidores a executar a ordem de atualização dos computadores, e não os utilizadores a decidir quando podem atualizar sistemas operativos dos computadores, ou mesmo Firmware dos computadores.

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, externos ou internos!

É também imperiosa a existência de »»

Lamentavelmente, teremos que admitir que, nos casos da INsegurança informática, a probabilidade de "nos bater à porta o infortúnio" é elevada, mas não temos que lhes facilitar a vida.

»»

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!

É absolutamente fundamental que, ao nível da camada de rede (switching e Wifi) existam Switch com inteligência e fiabilidade suficientes para implementação de políticas de VLAN, tantas quanto as necessárias, para, pelo menos, segregar os Turistas dos profissionais de Turismo. Há demasiados restaurantes, bares, agências de viagens e até hotéis sem que as redes Guest e Staff estejam separadas, pelo menos logicamente!

Uma rede sem VLAN é com uma porta sem chave.

É absolutamente indispensável criar e gerir acessos ao nível do servidor de ficheiros, com base em regras departamentais.

Pastas e ficheiros sem regras de acesso (leitura e escrita) é como uma porta sem chave.

A tradicional abordagem "coração que não vê, coração que não sente", do ponto de vista tecnológico, já não faz qualquer sentido, e ainda temos a legislação relacionada com o regulamento geral de proteção de dados que impõe procedimentos de salvaguarda e reposição dos sistemas dos players turísticos, por forma a 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...

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.

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. Para piorar o cenário, quando empresas enormes e de cariz fundamentalmente tecnológico, como as empresas de telecomunicações nacionais e internacionais ficam literalmente OFF durante mais de 48h, a probabilidade da coisa piorar é brutal... e ainda temos os drones, Internet das Coisas, e os carros autónomos...

Em jeito de conclusão, é sempre possível baixar o nível: há relatos de que as grandes multinacionais de reservas turísticas e hoteleiras 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...

...

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.

Enquanto profissionais de turismo, temos que:

1) 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) 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.
3) Auditar os sistemas e os processos de negócio que são suportados pelos sistemas informáticos da nossa organização, bem como o acesso dos nossos parceiros de negócio, (clientes ou fornecedores). **P**