O termo cybersecurity precisa ser incorporado ao seu escritório

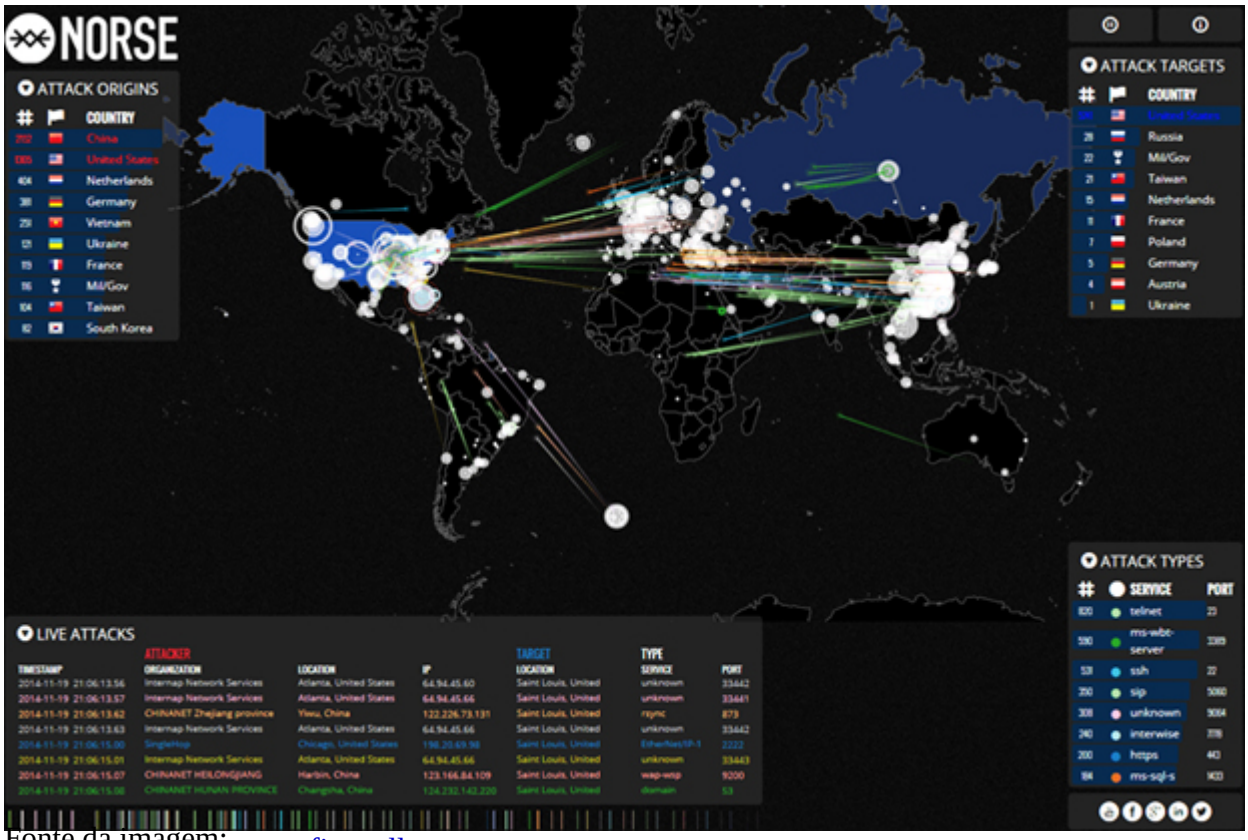
O ciberespaço é o ambiente formado pelos bilhões e bilhões de processadores interligados em nosso planeta (em alguns casos fora dele também). Neste ambiente está inserida a "Internet das Coisas", que liga seu carro ao seu celular e ligará sua geladeira ao seu nutricionista. Neste ambiente, está seu laptop de trabalho e o videogame de sua filha, juntos na mesma rede "segura" de sua casa.

Certa vez participei de um curso de Segurança da Informação no Centro de Análises de Sistemas Navais (Casnav) da Marinha do Brasil, unidade de excelência no assunto no país. Foi impossível não ficar espantado com a facilidade de capturar senhas em uma rede aberta (como um hotel por exemplo) ou de entrar na rede do vizinho com uma tabela com usuários e senhas padrão de fábrica dos principais roteadores disponíveis no mercado. Isso já faz tempo e hoje são erros que não acontecem mais, todos utilizam tuneis criptografados (VPN) ao acessarem seu e-mail em um hotel e todos trocam as senhas de fábrica nos equipamentos de sua casa. Em uma boa gíria para a situação: #sqn (só que não!).

Quem assiste a premiada série *Mr. Robot* pode ter ideia de como o assunto pode ser angustiante, além da sensação de que privacidade é uma ilusão.

Recentemente visitei um *data center*, local onde ficam armazenados dados de forma segura, algo como um cofre de dados, e no painel central com vários metros quadrados havia um mapa-múndi de monitoramento de ataques que mostrava em tempo real milhares de ataques acontecendo a equipamentos daquele tipo no mundo, uma verdadeira guerra mundial, como na figura abaixo.

www.firewall.cx



Fonte da imagem: www.firewall.cx

É claro que o assunto da segurança da informação não é novo, na verdade é milenar se pensarmos nas guerras e na espionagem. Ocorre que este tema e tornou fundamental nos escritórios de advocacia e nas profissões jurídicas, decorrente de uma sociedade hiperconectada e do uso obrigatório da tecnologia da informação como ferramenta de trabalho.

O impacto deste paradigma ainda está em construção do ponto de vista normativo, doutrinário e jurisprudencial, mas já pode ser sentido de forma avassaladora no emblemático caso do escritório panamenho Mossack & Fonseca, fonte dos dados do vazamento batizado de “Panamá Papers”.

Pense no impacto à imagem de seu escritório se todas as informações que um cliente lhe passou em confiança aparecessem disponíveis para download em vários pontos da Internet. Além da felicidade de uma eventual parte adversa, haveria uma possível responsabilização pelo vazamento em valores que poderiam ser impraticáveis.

A atualidade do tema no campo jurídico pode também ser verificada pelo movimento do provedor de conteúdo jurídico AML dos Estados Unidos. Esta organização edita diversos periódicos em nichos jurídicos, sendo o de maior interesse para esta coluna o *LegalTech News*. Eles também organizam feiras unindo tecnologia e Direito, sendo a maior a LegalTech de Nova York, já comentada anteriormente aqui na coluna.

Há pouco mais de um ano, a revista *LegalTech News* incluiu uma seção fixa sobre *Cybersecurity & Privacy* e há quatro meses vem editando um informativo (*newsletter*) pago sobre o assunto, o *Cybersecurity Law & Strategy Newsletter*. Interessante citar a frase de abertura da inscrição deste

informativo: "Não é se você vai ser hackeado, é quando."

E, exatamente hoje e ontem (27 e 28 de setembro de 2016), a AML está promovendo a segunda edição do evento cyberSecure, cuja lema é “o evento para crescimento e continuidade dos negócios”.

O evento trata desde a apresentação de tendências e tecnologias aplicáveis, até o uso de apólices de seguros para garantia quando do vazamento de dados. Um painel que chama a atenção pelo nome é, em tradução livre: “Escritórios de Advocacia: o elo fraco da defesa no ciberespaço? ” Indicando, possivelmente, os escritórios de advocacia como vetor de ataque dos hackers (crackers) para conseguirem de forma mais fácil e selecionada dados que estão mais protegidos e dispersos no ambiente do cliente.

Muitos poderiam dizer que este pensamento de defesa é uma paranoia quase desnecessária em escritório de pequeno porte, por exemplo. O cotidiano nos leva a sentirmos os procedimentos de segurança como obstáculos para a produtividade. Usar um duplo grau de ativação de um sistema de e-mails, recebendo um número de confirmação no celular a cada entrada no sistema, representa uma sensação de perda de tempo. A dosagem entre a produtividade e a defesa é um dos desafios do campo da segurança, não só da informação.

Na revista e informativo citados, por exemplo, alguns autores tratam o antes e o depois no Panamá Papers como mudança do paradigma para a mentalidade de segurança nos escritórios de advocacia.

A reflexão nos escritórios sobre esses assuntos deve levar em consideração assuntos como colaboradores, instalações e tecnologia, para os dados e para as comunicações.

Questões sobre onde os dados estão armazenados e quem tem acesso a eles? Ou, a segurança da nuvem versus as instalações do escritório? Não devem ser pesadas só pela visão da defesa, mas também sobre a sustentabilidade, como o backup para não perder dados e a disponibilidade para trabalho remoto e compartilhamento.

Melhor acessar ou levar um pendrive para casa? Uso o telefone ou o WhatsApp? São questões a serem combinadas no âmbito do escritório. Os usuários devem estar cientes sobre o que podem mandar por e-mail e por qual canal podem tratar de assuntos do cliente.

Essas reflexões levarão à necessidade de escolha de tecnologias e procedimentos. Procure profissionais para conversar sobre o assunto, afinal a informação é o mais valioso ativo de seu escritório e a consciência disto é uma tendência no campo jurídico.

Date Created
28/09/2016