



## >> O surfista e a onda: fraude na internet

O surfista desliza na onda, controla com mestria a deslocação da água e a força do seu movimento. É preenchido com uma sensação de domínio, capacidade de exercer poder e de disfrutar o prazer. No entanto, quando menos espera, é embrulhado e engolido por ela. Sacudido pela mesma força de movimento que acreditou controlar. É exatamente isto que ocorre com a internet e os seus utilizadores.

Foi há 23 anos, a 30 de Abril de 1993, que o CERN (Organização Europeia para a Investigação Nuclear) estabeleceu a internet (WWW - World Wide Web). Aconteceu o Big Bang da era da informação: a partir de então foi uma explosão de servidores e serviços com utilizadores a disponibilizar e a aceder à informação. O crescimento tem sido exponencial sendo a informação nela alojada, e os movimentos dos utilizadores enquanto nela navegam de enorme valor. Para além da informação per se, algoritmos sofisticados de big data conseguem encontrar e definir perfis de comportamento pela análise dos dados. A toda a informação recolhida pode juntar-se registo de local, dia e hora. Não há sector de atividade que não tenha sido penetrado pela tecnologia da internet.

World Wide Web, que se traduz literalmente em português por teia mundial, é uma autoestrada de informação, de fácil e rápido acesso. Hoje, há muitas empresas que apenas existem na WWW e modelos de negócio que se baseiam única e exclusivamente em plataformas web. A “uberização” ou economia colaborativa chegou e está a abalar os modelos de negócio vigentes, como sempre acontece com a integração de inovação tecnológica. Mesmo os mais reservados, já compram seguros na internet, usam home-banking, fazem compras sem verem diretamente os produtos, compram passagens aéreas e fazem as suas reservas de hotel. Comum a todas estas transações é a entrega de dados e, consequentemente, a partilha de informação relevante a propósito de cada um. O custo de tudo isto é a insegurança.

As empresas criadoras de software e hardware têm obviamente presente a questão da cibersegurança, mas é uma luta difícil de travar. Uma das formas de preservar a segurança é a de partilhar

as ameaças e os ataques, mas tal não ocorre como deveria por questões de receio de degradação de imagem e de perda comercial.

Os smartphones são muito mais do que telefones, são máquinas com grande capacidade de cálculo e de comunicação. Ao fazer uma chamada de A para B, um hacker pode passar a controlar e a recolher todo o conteúdo da conversa. O smartphone de B pode ser usado para atacar outros dispositivos escondendo a origem do ataque.

À medida que a computação se afasta dos computadores pessoais para a nuvem de dispositivos interligados e, com o potencial que tal acarreta na geração de mais dados, as preocupações com a segurança devem estar ainda mais presentes.

Talvez saibamos tudo isto, mas ainda não materializamos que estamos expostos mesmo quando julgamos que estamos a ser discretos. A câmara do nosso computador ou de um smartphone pode estar a captar tudo o que estamos a fazer. Com a incrível integração da tecnologia temos agora a chamada internet das coisas. O frigorífico recolhe e emite informação sobre o que consumimos, quantidades, tempo de uso. O televisor é um aparelho que além de receber canais de TV também emite informação para fora. As nossas fotos, vídeos estão armazenados na nuvem, sem sequer sabermos o local físico onde estão. Por exemplo se usarmos software da Google, e estando na Europa os nossos dados podem estar ou na Irlanda (Dublin), ou na Holanda (Eemshaven), ou na Finlândia (Hamina), ou ainda na Bélgica (St Ghislain). Mas o que podem fazer com as nossas fotos? Muita coisa ... E sim, é lá algures que estão os nossos dados. E sim, mais dados nossos noutras empresas estarão noutros locais, e bem remotos.

Bases de dados com informação relevante e confidencial podem ser acedidas para venda e uso por empresas para qualquer fim. Frequentemente são reportados roubos de bases de dados de empresas que gerem as nossas caixas de correio eletrónico, de acesso ilegítimos a bancos, a companhias de seguros e hospitais. Dados hospitalares podem interferir com a atividade seguradora. A manipulação de dados bancários é uma devassa e pode ter consequências legais e criminais mas também de chantagem.

A encriptação de mensagens está na ordem do dia. Do ponto de

vista da segurança das comunicações é sem dúvida a melhor solução possível, tornando, pelos padrões atuais, quase impossível descriptar. Por outro lado, esta segurança impede a pesquisa de comunicações suspeitas e fraudulentas. A velha dicotomia segurança e liberdade.

Mas o pior é que temos práticas pouco cuidadas que fazem com que seja cada um de nós o nosso maior inimigo. Sim, a maior ameaça à segurança não são os piratas informáticos, nem organizações criminosas sedentas de dados para manipulação e venda, nem estados para controlar os seus cidadãos ou outros estados. A maior ameaça somos nós. É cada um de nós, ao clicar em links sem razão que não seja por puro voyeurismo ou ao abrir inadvertidamente ficheiros com a gula de obter algo de forma fácil e sem custos. Basta um destes ímpetos para se expor uma porta de vulnerabilidade dando origem ao saque de dados e à sangra de privacidade.

De momento, as melhores práticas parecem ser, para além do bom senso e juízo na utilização da tecnologia, a manutenção dos equipamentos o mais atualizados possível para que falhas de segurança vão sendo reparadas.

Não obstante as fantásticas capacidades e oportunidades que a internet nos trás, não devemos esquecer que é uma montra que nos expõe e que tem a força da onda que nunca dominaremos. Procuramos exposição nas redes sociais para impressionar, para mostrar os nossos feitos tentando esconder os defeitos, para criar um perfil de intervenção nas coisas quando somos passivos a intervir nas causas. Para nela surfar é fundamental que nos conheçamos a nós mesmos.

Nas palavras de Mia Couto, "Nunca o nosso mundo teve ao seu dispor tanta comunicação. E nunca foi tão dramática a nossa solidão. Nunca houve tanta estrada. E nunca nos visitamos tão pouco."