

«Porque importa a segurança da Internet?»¹

Nos dias de hoje, agora que a *Internet* é parte integrante das nossas vidas, facilmente nos esquecemos de que há 15 anos, pelo menos para a maioria das pessoas, nem sequer “*existia*”. Em abono da verdade, quanto à *Internet*, desde a sua iteração inicial como veículo de troca de mensagens entre académicos e cientistas, já passaram 45 anos.

Mas então, como se explica o crescimento da *Internet*, desde essa origem «académica» até à sua indispensabilidade global dos dias de hoje? Muitos dirão que este crescimento se deveu à criação da *WWW* (*world wide web*) ou à velocidade de transmissão de dados que permitiram a sua acessibilidade a biliões de utilizadores.

Eu, porém, arguirei que se deve a um outro factor – embora menos visível, mas igualmente crucial – a Segurança. A segurança da informação, enquanto garante da privacidade, autenticidade, integridade e disponibilidade. Sem ela, todas as transacções eletrónicas, desde pequenas compras com cartão de crédito a transacções de biliões de dólares, não aconteceriam. Até as mais simples interações pessoais, nas nossas vidas em rede, seriam largamente perturbadas se não pudessemos proteger os nossos dados pessoais.

Hoje em dia, a concepção da rede altera-se a uma velocidade como nunca antes vista : de conexões sem fios a uma imensa e invisível rede, o número de telemóveis, por exemplo, com acesso à *Internet* é aproximadamente o mesmo que o número total da população mundial. Mais, no presente, carros e televisões são já fabricados com capacidades embutidas de acesso à rede, seguindo-se uma infinidade de frigoríficos, torradeiras, aquecedores, ares-condicionados, iluminação, "inteligentes"... No curto prazo poderemos ter mais aparelhos do que computadores *online*.

Acredito que o problema não esteja na ampliação do escopo da própria tecnologia de base, mas na forma indiscriminada de o fazer. Ainda que a segurança seja peça-chave da afirmação e crescimento da tecnologia e da rede nas duas últimas décadas, a minha preocupação prende-se com o facto de se lhe não reconhecer essa crucialidade, e assim, descurar-se a sua presença nos novos produtos e sistemas criados a partir do zero. Ao invés de o factor «Segurança» ser encarado como uma prioridade do *design*, este é adicionado aos produtos *à posteriori*, e, mais das vezes, de forma negligente. E isto assim não é apenas má planificação; é a receita perfeita para o desastre.

De certa forma, admito a segurança da Internet em condição terrível. Eu sei que parece soar alarmista, mas a verdade é, no imediato, bastante ensurdecadora : a pirataria, de indivíduos, de organizações e de governos, mostra-nos um fluxo constante. Há, a este título, uma piada no mundo corporacional, lapidar: «*No mundo dos negócios existem apenas dois tipos de empresas: as que foram invadidas e as que não sabem que o foram.*» Mesmo assim, apesar disto, muitas grandes

¹ Tradução por Nuno Teixeira Castro

organizações ainda consideram a cibersegurança como uma prioridade de nível inferior, uma rubrica de despesa a ser minimizada sempre que possível. O paradigma permite-nos constatar que as empresas investem mais tempo e esforço na concepção dos seus edifícios «*amigos do ambiente*» do que em proteger as suas redes de tecnologia da informação.

Como resultado, umas atrás das outras, vamos conhecendo situações de infiltração na rede, roubo de informação privilegiada, e até de danos físicos. Mais, por razões legais e de confiança, muitas organizações não divulgam os ataques de que são alvo, por forma a mitigar a percepção geral do risco. A realidade, dura, permite-nos assistir a constantes violações de propriedade intelectual de todos os tipos, de dados confidenciais dos governos a dados pessoais de clientes organizacionais, até à chantagem exercida sobre um grande estúdio de cinema de *Hollywood*. Em minha opinião, neste caso, o roubo de *Terabytes* de dados da *Sony Pictures* não é tão alarmante como a facilidade com que os *hackers* invadiram o sistema e roubaram os dados sem que ninguém tivesse percebido.

No mundo real existem milhares de empresas como a *Sony Pictures* - respeitáveis, organizações sérias, que compraram algum pacote *off-the-shelf* de segurança de TI ou contrataram alguma empresa especializada para gerir a sua segurança *online*. Não obstante, podemos afirmar que, no futuro, conheceremos *hacks* tão graves, pelo menos, como o da *Sony Pictures*. E o risco associado extravasa largamente a mera questão da perda de informação: as organizações correm o risco da perda de reputação, da baixa de produtividade e de moral dos seus funcionários e, claro, ações judiciais em catadupa de acionistas e parceiros de negócios. Nos próximos anos, a repetição da pirataria das organizações irá afetar drasticamente o ambiente do mundo dos negócios.

Impõe-se um reexame imediato à segurança da Internet antes que as coisas piorem. Especificamente, é necessário realizarmos um debate verdadeiramente multissetorial capaz de coordenar, quer setores públicos quer privados, a uma amplitude sem precedentes. Isto exigirá a cooperação de algumas organizações que ainda não realizaram atividades de colaboração na resolução destas questões globais. Por razões óbvias, acredito que não há plataforma melhor posicionada do que o Fórum Económico Mundial para levar a cabo esta difícil tarefa.

Se não lidarmos com este problema, os riscos manter-se-ão enormes. Numa cadeia de perda de confiança, primeiro as organizações e, de seguida, o público tenderá a perder a fé em tudo o que vê nos seus monitores, e a *Internet* deixará de funcionar como, talvez, a ferramenta mais utilitária alguma vez criada.

Autor: *William H. Saito* é Consultor especialista no Gabinete do Governo do Japão. É também um *Young Global Leader* e membro do *Forum's Global Agenda Council (Cyber Security)*.