NOVO PRODUTO: RISCOS CIBERNÉTICOS

O FUTURO É HOJE

Antigamente, muitos dos atos que hoje fazem parte do nosso cotidiano ou rotina diária provavelmente seriam considerados pura ficção científica. Pedir ao carro que ligue para casa, desbloquear o celular utilizando a impressão digital ou guardar todos os arquivos em uma nuvem digital, são alguns dos vários exemplos que hoje nos parecem normais e que, "pouco tempo atrás", teríamos pensado que fariam parte do roteiro de *Homens de Preto*.

As novas tecnologias avançam a uma velocidade vertiginosa, e o mundo avança com elas. Afetam todos: pessoas, governos, pequenos comércios e grandes corporações, além de terem mudado completamente a forma como nos relacionamos. Desde os aplicativos de mensagens instantâneas à apresentação telemática de documentos oficiais, passando por todas as plataformas ou redes sociais. Alguém se lembra dos ultraleves sobrevoando as praias com anúncios pendurados?

Todos os avanços tecnológicos têm, como norma geral, um princípio ou denominador comum, e são criados para tornar muitas das tarefas dos homens, dos animais e da natureza mais fáceis, mais rápidas e (muitas vezes) melhores.

Essa afirmação, a princípio positiva, leva também a outra reflexão fora das discussões éticas: Novos cenários, novos riscos.

O cenário patrimonial das empresas mudou de forma significativa. Os bens intangíveis têm um peso e uma

relevância cada vez maiores em relação aos bens tangíveis. Essa mudança exigia uma substituição do papel do seguro tradicional, que estava centrado em oferecer soluções, principalmente na transferência de riscos sobre os bens tangíveis, deixando um vazio significativo quanto aos intangíveis.

A velocidade à qual as mudanças nos cenários são provocadas fizeram com que a percepção dos novos riscos, que poderíamos chamar de "riscos cibernéticos", se afastasse do seu alcance real.

Atualmente, podemos dizer que, no âmbito das grandes multinacionais, essa distância começou a diminuir. Na última pesquisa realizada no World Economic Forum sobre os principais riscos que afetam a economia, os ataques virtuais já se situam entre os cinco mais preocupantes.

Em artigos publicados recentemente nos meios especializados, percebe-se um discurso mais maduro dos principais Risk Managers europeus. Nesse sentido, manifesta-se a necessidade de uma conscientização ampla por parte da empresa da qual a diretoria executiva participe ativamente. Por outro lado, exige-se da indústria de seguros soluções sob medida que se adaptem à complexidade dos novos riscos. Já não podemos nem devemos falar de um risco emergente, nem de um problema limitado às áreas de TI das empresas. Estamos em uma fase em que tanto os Brokers quanto as empresas de seguros e os Risk Managers começam a se coordenar e são obrigados a se entender.

O crescente número de ataques cibernéticos (a Espanha é o terceiro país do mundo, atrás dos EUA e do Reino Unido) nos quais são geradas perdas anuais para as empresas acima de 14 bilhões de euros, bem como o considerável aumento de custo médio por incidente, que passou de 0,5 milhão de euros em 2012 para 0,8 milhão de euros em 2013, com um custo médio anual, por empresa, de quase 9 milhões de euros, estão transformando os investimentos em tecnologia em um dos itens prioritários das agendas das empresas, embora ainda haja um longo caminho a ser percorrido no que diz respeito às pequenas e médias empresas.

Nesse sentido, segundo o Cost of Cyber Crime Study, publicado pelo Instituto Ponemon em 2014, manifesta-se o alto retorno sobre o investimento nas principais tecnologias de segurança, tais como sistemas de encriptação (18%), sistemas de inteligência em segurança (21%) ou perímetros avançados de controle de firewall (15%).

A maioria dos sinistros de grande intensidade provém do mercado norte-americano (Target, Anthem, Home Depot), sendo derivados principalmente de violações de seguranças que afetam grandes bancos de dados pessoais.

Vale ressaltar que o mercado norte-americano foi pioneiro nas coberturas de riscos cibernéticos como resposta às particularidades das normas locais que regulam as indenizações relacionadas à proteção desses dados.

No caso concreto do Target, uma das maiores redes de supermercados dos Estados Unidos, que teve dados financeiros e pessoais de 110 milhões de clientes roubados por delinquentes virtuais que entraram nos sistemas da empresa através de um pequeno fornecedor de serviços de refrigeração, manifestou-se a necessidade de contar não só com medidas de segurança próprias, mas também com a necessidade de garantir que os fornecedores que tiverem acesso a informações sensíveis tomem as mesmas medidas.

Não obstante, além das peculiaridades do mercado nos Estados Unidos, considerando-se as consequências derivadas das ameaças virtuais, o impacto gerado pela interrupção de negócio nas empresas exige cada vez mais atenção. A operação da grande maioria das empresas depende, principalmente, de seus sistemas informáticos. Um ataque ou uma falha nesses sistemas pode provocar um verdadeiro caos interno, possivelmente contagiando os mercados. Assim, todas as medidas de segurança não devem ser orientadas apenas para a proteção de informações sensíveis, mas também para proteger e garantir a continuidade do negócio.

A variedade de agentes que formam o quadro de ameaças virtuais (espiões, delinquentes, hacktivistas, terroristas ou, inclusive, os próprios funcionários das empresas) e a crescente sofisticação das ferramentas e dos métodos de ataque utilizados por eles (phishing, malware, exploits…) colocam todos em perigo. Há poucos dias, foi publicado que hackers"assaltaram" os bancos de dados da Agência de Pessoal do Governo dos Estados Unidos e coletaram uma quantidade considerável de dados pessoais de funcionários federais.

Diante desse panorama, apesar de estarmos em uma etapa que está avançando do ponto de vista legislativo para se adaptar a esses novos cenários, a palavra-chave a ser destacada é "prevenção".

Como mencionado anteriormente, o desenvolvimento do papel da indústria de seguros na prevenção desses novos riscos representa uma oportunidade de negócio, sendo que as empresas que souberem ouvir e se adaptar melhor às necessidades do cliente terão uma vantagem competitiva.