MAIS
SEGURO

Unsplash

Como se defender e mitigar riscos perante um ataque cibernético

Num mundo globalmente digital os ataques cibernéticos estão na ordem do dia e os seguradores continuam a estudar as consequências e a forma de mitigação. Há já soluções para grandes companhias,PME e famílias. A assunção de que existe um risco latente para uma simples família ou para uma empresa de reduzidos recursos ainda é um problema considerável, alertam os especialistas consultados. Os ataques cibernéticos são complexos, podem envolver Estados e criar confusões a nível global, ou podem constituir formas simples de extorsão. Entre as diversas estratégias usadas, alerta o broker MDS, estão os esquemas de fraude online e phishing, através dos quais o hacker, "fazendo-se passar por entidades governamentais e de saúde, utiliza o tema do covid-19 como isco para obter de forma fraudulenta dados pessoais e/ou descarregar conteúdo malicioso". Outro ataque em destaque é a utilização de software malicioso (malware, ransomware), onde códigos informáticos são utilizados para atacar sistemas e infraestruturas informáticas de organizações, dos quais pode resultar o bloqueio de sistemas, das operações, ou mesmo gerar perda de informação. "Adicionalmente, são ainda de referir o ataque de negação de serviço (DDoS), um estratagema mediante o qual o criminoso intencionalmente sobrecarrega o servidor, site ou rede de um terceiro com o objetivo de o paralisar; bem como os domínios de internet falsos, em que o hacker, também utilizando o tema covid, cria domínios/sites falsos para tirar vantagem da pesquisa de informação dos utilizadores para desenvolver ataques, como sejam o phishing e o malware". E quais são as soluções? É preciso saber transferir riscos e isso implica seguros mas também serviços prestados por especialistas em riscos cibernéticos. O mesmo broker dá o exemplo das "diversas garantias de danos e prejuízos sofridos pela própria empresa, nomeadamente: custos com investigação forense; custos incorridos para substituir, restaurar ou recuperar dados; perdas de lucros por interrupção; custos de notificação de violação de dados; gestão de eventos de extorsão e roubo de identidade; danos reputacionais. Incluem ainda a cobertura pela subtração de fundos via transferência eletrónica (crime cibernético); a responsabilidades perante terceiros lesados; e, serviços adicionais focados na prevenção, monitorização, atendimento imediato pós-evento e serviços especializados de informática forense". Estas soluções já estão disponíveis em Portugal e para o cálculo dos custos é relevante a faturação, o número de empregados e/ou utilizadores, o sector de atividade ou os capitais. ●

OPINIÃO

O avanço tecnológico e a sofisticação da arte da manipulação em rede

DUARTE ANDRÉ LIMA
Web/Frontend Developer

O avanço tecnológico aproxima-nos dos serviços que mais usamos no dia-a-dia. A cibercriminalidade afasta-nos da sua utilização. Será este avanço tecnológico seguro para quem o usa?

Com o avanço da inteligência artificial e o desenvolvimento tecnológico, os hackers foram aprimorando as suas técnicas. Os métodos clássicos como o phishing ou o malware estão ultrapassados no tempo e apesar de muitos recorrerem ainda à famosa técnica do mail "encriptado" o mesmo já não contém um ficheiro para o incauto descarregar, mas sim uma réplica de um browser funcional. Esta réplica terá o mesmo aspeto e funcionará da mesma forma que um browser genuíno, mas terá, com certeza, outra intenção. Quando o utilizador se apercebe deste intruso, se chegar a perceber, já será tarde. A tecnologia swarm e o 5G são dois avanços tecnológicos com o intuito de simplificar operações digitais. A primeira consiste em sistemas descentralizados que usam a automação para operar, não necessitando de intervenção humana. Aquando usada por hackers, swarm bots podem penetrar uma rede e derrubar as suas defesas para a obtenção de dados. Eventualmente, estes mesmos bots - aplicações autónomas espalhadas por toda a internet com um determinado propósito - terão a capacidade de partilhar e correlacionar a informação obtida em tempo-real e modificar o ataque a determinado alvo desejado. A juntar a este cenário está o 5G, que pode ser o catalisador para um maior número de ataques swarm. Um hacker ao transformar inteligência e velocidade do 5G e tecnologia de ponta em armas digitais, consegue usar qualquer dispositivo eletrónico como um condutor de código malicioso - código desenvolvido pelo hacker que lhe permite ter acesso a computadores de terceiros - com o propósito de impulsionar os seus ataques informáticos.

Os bots são uma novidade tecnológica e, para muitos, uma arma cyber. Tão-só um bot não faz muitos danos, mas se for uma rede deles (botnet) o poder e a perigosidade aumentam exponencialmente. Um botnet possibilita a um hacker sobrecarregar os recursos de um determinado alvo ao ponto do mesmo ficar offline originando perdas monetárias e de clientes. A sua eficácia, o seu custo reduzido e a facilidade de criação faz com que este tipo de ataques sejam cada vez mais frequentes.

Alguns países com os seus recursos ilimitados lideram a corrida ao desenvolvimento de novas ferramentas de ataques informáticos que, por sua vez, são usados para desenvolver outras ferramentas e novos tipos de ameaças informáticas. O ataque WannaCry ocorrido em 2017 e protagonizado pela Coreia do Norte que atingiu produtos windows em 150 países e gerou perdas de milhões de milhões de US dólares é um exemplo inequívoco da sofisticação dos métodos usados por estes países. A tendência é, cada vez mais, a demonstração do poder através de ataques em rede, altamente nefastos.

A crença de que as grandes empresas são o alvo principal do ciberterrorismo não é rigorosa. São exatamente as pequenas e médias companhias que, pelo facto de não terem tanta disponibilidade financeira para apostar em segurança de última geração, se tornam uns alvos para os piratas informáticos e, muitas vezes, o ganho é superior ao das grandes empresas. ●

ANÁLISE

Ciberataques. Um fenómeno para ficar e que o contexto pandémico ajudou

Os seguradores ainda têm muito trabalho pela frente. Até perceberem como podem mitigar riscos e os segurados (clientes), terão de perceber que a proteção tem um custo.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

O que está por detrás dos ataques cibernéticos? As motivações podem ser políticas, religiosas ou outras, diz Jorge Tobias, responsável de Riscos Cibernéticos da Willlis Towers Watson. Descarta que tenha sido a pandemia a exacerbar esses ataques, embora existam exceções nesta leitura como foi o caso recente sobre a tentativa por parte de hackers russos de tentarem aceder a informação sobre o desenvolvimento de vacinas para a Covid-19 no Reino Unido. Ideia semelhante é defendida por Pedro Pinhal, diretor de Sinistros da MDS Portugal que afirma que "após o início da pandemia, assistimos a uma maior preocupação das famílias e empresas relativamente ao risco cibernético. De facto, apesar da consciência para os riscos cibernéticos ser, ano após ano, cada vez maior, a atual pandemia elevou este tipo de riscos a um patamar nunca antes visto. E atingiu de forma transversal toda a sociedade, isto é, cidadãos, famílias e organizações, sejam elas de pequena, média ou grande dimensão. Esta maior preocupação tem fortes motivos para se verificar pois, como revelam os mais recentes dados, o número de incidentes em Portugal e no mundo tem assumido proporções nunca antes vistas. Por exemplo, segundo os dados mais recentes do Gabinete de Cibercrime da PGR, nos primeiros cinco meses deste ano tinham sido registadas mais 139% de denúncias de crimes cibernéticos do que em todo o ano de 2019!" E claro que a necessidade de reduzir o risco de contágio do vírus alterou a forma como se trabalha, como estudamos ou como comunicamos, tanto em casa como no trabalho. Todos nós nos tornámos fortemente dependentes dos sistemas informáticos. Diz Sjoerd Smeets, *chief risk officer* do grupo Ageas Portugal

O número de ataques de spam, phishing e malware está a aumentar muito (pelo menos em 35%)

que a mudança do modelo de trabalho foi súbita e nem todas as empresas tiveram tempo de implementar os mecanismos de segurança adequados para os seus colaboradores.

Muitos destes nem estavam completamente cientes de todos os riscos cibernéticos. Smeets frisa que "os cibercriminosos estão a tentar explorar esta vulnerabilidade e o número de ataques de spam, phishing e malware está a aumentar muito (pelo menos em 35%). É crucial que todos estejam bem cientes dos riscos que correm, e que utilizemos a internet de forma mais responsável, com proteção e de forma a reduzir os riscos de ciberataques".

A digitalização dos negócios, e da vida humana em geral, é a grande razão pela qual os ataques acontecem e têm um impacto brutal, diz Manuel Coelho Dias, Cyber Risk Specialist da Marsh Portugal. Acrescenta que "a partir do momento em que grande parte do valor de uma empresa se encontra digitalizado (sejam segredos de negócio, bases de dados de clientes, contactos de fornecedores, mas também a operação em si e a cadeia logística), os ativos digitais tornam-se uma camada de valor muito assinalável e apetecível aos criminosos. As grandes tipologias de eventos que têm afetado as empresas são os *data breaches* em que há mera extração das bases de dados, os ransomwares (nos quais pode ou não haver extração das bases de dados hackeadas), o spear phishing e as fraudes por engenharia social. De acordo com a informação coligida pela Marsh, CMS & Wavestone no The Changing Face of Cyber Claims Report, os ransomwares são a ameaça mais frequente na nossa carteira de clientes, mantendo uma tendência de subida muito assinalável nos últimos anos".

E o que vai mudar? No seguros o novo foco está na proteção cibernética e potenciais coberturas para a interrupção temporária de negócios. No entanto, a maior mudança será na transformação digital, refere o mesmo gestor. E adianta que esta pandemia acelerou esse processo. Nas vendas, os canais digitais estão a ganhar relevância, mas também os canais mais tradicionais como os mediadores ou o canal bancário tiveram necessidade de se reinventar e apostar em ferramentas digitais como suporte ao negócio. Ao nível dos sinistros, os clientes não precisam de se deslocar a uma oficina para fazer a peritagem ao veículo em caso de acidente, podem fazê-la na comodidade da sua casa, garagem ou escritório. E nos seguros de saúde, os clientes começaram a utilizar soluções de telemedicina. Por sua vez, Manuel Moita de Deus, da NacionalGest, realça que quase se analisa o setor financeiro e a indústria seguradora em particular "há algo de fundamental e transversal: a total dependência da base de dados de clientes e a inexistência de produtos físicos em armazém". ●

ENTREVISTA ALEXANDRE RAMOS **Membro da Equipa Executiva e WEM Technology Leader da Liberty Seguros**

Liberty cria ecossistema na 'cloud' pública

Construir um seguro à medida de cada um e uma oferta personalizável é o objetivo da Liberty Seguros com um novo ecossistema, afirma Alexandre Ramos, da área tecnológica da companhia.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

O que ganha a empresa e o consumidor com a recente decisão de construção de uma cloud pública sem ligação ao ecossistema existente?
A criação de um ecossistema digital na cloud pública permite-nos alterar a forma como trabalhamos, sermos mais ágeis em satisfazermos as necessidades dos nossos clientes e em darmos resposta aos nossos parceiros de negócio e mediadores, ao mesmo tempo permanecendo competitivos, enquanto criamos um ambiente de trabalho mais dinâmico para todos. Esta transformação implica uma adaptação de todos no curto e médio prazo, mas, a longo prazo, veremos como o nosso trabalho se transforma na sua versão mais eficiente, obtendo mais tempo e recursos para nos dedicarmos a darmos o melhor de nós aos nossos parceiros estratégicos e subsequentemente aos nossos clientes. Assim que se atinja a maturidade de capacidades e linhas de negócio, bem como serviço a clientes e agentes, o crescimento estimado será sempre de dois dígitos.
Por seu lado, os consumidores passam a ter uma oferta totalmente personalizável, ajustada às suas necessidades, uma vez que todas as coberturas dos nossos produtos passam a ser opcionais. Ou seja, os clientes vão poder construir um seguro à sua medida, escolhendo aquilo que desejam incluir na sua proteção.

Não são esperados bugs na migração?
Quando se embarca numa jornada como esta, onde o mindset é arriscar e aprender e corrigir rápido, os erros aparecem. A diferença é que a nossa capacidade de os resolver rapidamente é substancialmente maior. Além disso, a Liberty tem longa experiência em migrações, em todo o mundo, pois temos uma equipa muito experiente a um nível global, criamos parcerias fortes com entidades que têm ainda mais anos de experiência do que nós, e temos um ecossistema ágil que nos permite corrigir desvios muito mais rapidamente. Se podemos prometer perfeição, isso claramente ninguém pode, mas podemos prometer planeamento cuidado, estratégia robusta e execução o melhor possível, isso claramente.

Que investimento foi feito e onde estão as grandes novidades tecnológicas?
A criação deste ecossistema digital é o nosso maior investimento nos últimos anos. É um novo modelo de negócio, que estamos a implementar com base na criação do nosso próprio ecossistema tecnológico na nuvem pública. Este ecossistema está e vai dar-nos maior agilidade no design de novas coberturas de riscos, para que possamos oferecer mais tempo de análise das necessidades de cada cliente. Estes vão poder construir um seguro à sua medida, escolhendo aquilo que desejam incluir na sua proteção. Apostou-se em tecnologia baseada em cloud, modular e completamente orientada a API's. Permitindo deste modo evoluir a tecnologia sempre que necessário e de acordo com a inovação que vai aparecer frequentemente. Tudo isto com evoluções das PaaS, SaaS mensalmente e de forma transparente, evitando deste modo as práticas passadas de ter que se investir tempo e recurso a evoluir soluções, criando grande impacto no negócio.
Além disso, passámos de processos de criação de produtos ou políticas que podem levar até um ano a serem implementados, para um modelo de criação de coberturas modulares personalizáveis, que podem ser disponibilizadas ao cliente em apenas 48 horas.

A segurança do sistema a viver na cloud é de 100%?
Sim. Por um lado, os dados que estão a viver na cloud estão salvaguardados com certificações externas (e.g. Verizon) através de práticas e tecnologia que asseguram elevados níveis de segurança; por outro lado, usamos práticas instituídas pela Amazon Web Services (AWS), que está a colaborar com a Liberty neste projeto e que certifica que os dados estão protegidos. Além destas medidas, as plataformas estão de acordo com as normas RGPD e os seus guidelines.

ALEXANDRE RAMOS
Membro da Equipa Executiva e WEM Technology Leader da Liberty Seguros

Como é ultrapassada a barreira da língua, da conversão da moeda, das diferentes envolventes normativas e regulamentares e a necessidade de controlo do branqueamento de capitais?
Esta nova infraestrutura vai eliminar os sistemas e data centers existentes. Com base no conceito de modularidade de rede, passamos de um greenfield para uma solução completa, na qual os produtos e serviços podem ser lançados sem restrições de idioma, moeda, geografia ou contexto específico de cada mercado. Estes vão facilitar um modelo operacional mais simples, principalmente em relação aos produtos low touch e no touch.

Qual a reação do regulador português a esta iniciativa?
O mercado segurador tem evoluído digitalmente nos últimos anos, assim como outras indústrias, sobretudo para responder às necessidades dos clientes, num ambiente omnicanal, para que possamos comunicar de forma cada vez mais simples, rápida e eficaz entre todas as partes – seguradora, mediadores e clientes. Na Liberty estamos a aproveitar a transformação digital para reforçar o posicionamento como uma empresa inovadora, revolucionária e pioneira na forma como oferecemos seguros e respondemos às tendências, estando presentes onde o cliente precisa de nós, a partir de qualquer canal. Queremos estar entre as 10 maiores companhias de seguros da Europa. ●

INOVAÇÃO

F. Rego lança produto para doenças graves

A corretora F. Rego vai lançar um produto segurador destinado a cobrir doenças graves em adultpos e crianças.

O novo produto da F. Rego tem duas grandes modalidades, sendo que para os mais jovens poderá ser contratualizado com um custo a começar nos quatro euros/mês, sendo que nas crianças e jovens (entre os 30 dias e os 17 anos), esta solução pioneira prevê o pagamento de uma indemnização perante o diagnóstico de um conjunto de doenças consideradas graves, nomeadamente o AVC, o transplante de um órgão vital, o padecimento de cancro ou diabetes tipo I, sendo esta última cada vez mais comum. Já para os adultos (entre 18 e 64 anos) existe a possibilidade de contratação da mesma solução, com um painel diferente de patologias, nas quais se destacam o cancro, o enfarte do miocárdio, o AVC, a esclerose múltipla, a insuficiência renal terminal e a necessidade de transplante de órgãos vitais, entre outros. Pedro Rego, CEO da F. REGO, explica que "este é um produto que se traduz num verdadeiro e eficaz apoio às famílias, disponibilizando a verba contratualizada perante a existência de diagnóstico, e permitindo à família uma gestão livre da mesma, com a adequação que entender mais adequado ao doente". Afirma ainda que "não se trata de um concorrente aos seguros de saúde, mas sim um complemento dos mesmos, respondendo de forma mais ampla ao que são as necessidades decorrentes de enfermidades desta gravidade." ●

ANÁLISE

O mundo pós Covid-19 obriga a preservar a identidade digital

Cada vez mais vai ser necessário termos cuidado com a nossa identidade digital, afirma Nuno Albuquerque e Castro, da área de seguros da everis Portugal.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

"O confinamento originado pelo covid veio incrementar, em grande parte das empresas, a necessidade de digitalizar atividades da sua cadeia de valor para proteger os seus colaboradores e para poderem continuar a servir os seus clientes durante este período", afirma Nuno Albuquerque e Castro, responsável pela área de seguros da everis Portugal. Adianta que o mundo pós Covid "é e será certamente mais digital. Estudos recentes afirmam que no espaço de dois meses a adoção de ferramentas e instrumentos de interações digitais acelerou em mais de cinco anos. Assistimos a seguradoras a transitarem as suas equipas de suporte ao cliente para formato totalmente remoto, escolas a utilizarem salas de aulas digitais, médicos a prestarem cada vez mais apoio especializado de forma totalmente online, os exemplos são infindáveis". Adianta que todos estes fatores despoletaram uma mudança e intensificaram a forma como nos relacionamos com a tecnologia, "permitindo a consumidores e empresas entenderem a preponderância que esta tem nas nossas vidas diárias e a explorarem formas alternativas de a utilizar". Os serviços numa perspetiva tradicional, só existem e criam valor se resolverem problemas concretos nas jornadas dos clientes (sejam estes B2C ou B2B). Como tal, o mundo pós covid criou a necessidade de existir uma restruturação do que são os problemas a resolver, as estruturas de custos que as organizações possuem e que novos modelos de negócio podem existir.

E sobre os seguros, para além do evidente aumento de pontos de contacto digitais B2C e B2B, "destaco tudo o que esteja relacionado com a infraestrutura digital, seja de cada um de nós ou das organizações. Cada vez mais, vai ser necessário termos cuidado com a nossa identidade digital ou de manutenção do que é a nossa infraestrutura como organização. A aceleração da utilização dos mecanismos digitais obrigará à existência de componentes que assegurem a continuidade das várias atividades. Ou seja, novos riscos obrigarão a novas produtos/soluções para a indústria seguradora. Por exemplo, temos assistido cada vez mais ao lançamento de novas soluções cyber que nos permitem proteger a nossa informação seja no contexto pessoal ou no contexto profissional".

Por outro lado, o comportamento do consumidor à data de hoje já é diferente, diz o gestor. Por exemplo, "há várias atividades que sofreram grandes alterações em termos de consumo: compras online; exercício em casa; trabalho remoto a 100%. Estas tendências serão acentuadas pelo impacto económico que esta pandemia terá. As organizações vão precisar de ajustar os seus produtos/serviços às novas jornadas do cliente, seja por estas alterações ou pelos impactos económicos que obrigarão os consumidores a focarem-se nos produtos essenciais. Assim, é provável que o consumidor valorize muito mais um produto ou serviço que consiga cumprir a sua função essencial no contexto correspondente valorizando a confiança que deposita numa determinada marca".

E sobre o futuro e o crescimento da economia diz que a aposta no "Green Deal" é a resposta que a UE coletivamente escolheu para tentarmos manter o bem-estar de todos os europeus. Ou seja, "os investimentos públicos necessários para tentar reduzir o impacto económico que a Covid criou, irão focar-se em ganhos de médio e longo prazo e numa forma de estar diferente. Mais recentemente a criação do Banco de Fomento em Portugal para financiar projetos sustentáveis de neutralidade carbónica e de economia circular é um excelente sinal de apoio e promoção de investimentos públicos".

Por outro lado, "as relações sociais estão a ser certamente afetadas", adianta. Apesar das interações serem cada vez mais digitais, "nem o contacto físico, nem as nossas identidades em cada um dos grupos que pertencemos são passíveis de ser substituídas. No contexto empresarial os contactos presenciais continuarão ser preponderantes para manter e promover a cultura, valores e o ADN da companhia. Do meu ponto de vista, não deveremos confundir distanciamento físico de distanciamento social. Infelizmente, as palavras que foram escolhidas para descrever o atual momento não foram as melhores, pois dão a entender que nos devemos isolar socialmente o que está errado". ●

OPINIÃO

Seguros e a Covid-19: do problema à solução

PEDRO REGO
CEO F. REGO – Corretores de Seguros

Enquanto indústria que tem no risco o *core* da sua atividade, é compreensível que o setor segurador esteja continuamente exposto ao escrutínio e à crítica. Este é um exercício importante, que promove a transparência e o rigor da sua atuação. Considero, contudo, que não se dá o devido valor à função social deste setor, responsável pela devolução à economia de 13,6 mil milhões de euros (2018) por via do pagamento de sinistros, impostos e salários, além de se assumir como um dos principais investidores institucionais da economia portuguesa.

Concluído o primeiro semestre do ano (e registe-se que nos dois primeiros meses do ano, no mundo ocidental, a atividade económica não esteve condicionada), estima-se que as perdas diretas globais da indústria seguradora atinjam já os 17,6 mil milhões de euros. Este é um impacto transversal às seguradoras e resseguradoras, bem como às diferentes geografias, e que se estima que venha a aumentar, devido à redução da atividade económica de indivíduos e empresas e ao agravamento das catástrofes naturais.

Se é verdade que determinadas apólices, como a do seguro automóvel, viram o período de confinamento reduzir substancialmente a sua exposição ao risco, não é menos assertivo afirmar que estes ganhos são manifestamente insuficientes para cobrir os prejuízos relacionados com o cancelamento de eventos e de viagens, bem como as perdas nas áreas do crédito e caução, interrupção de negócio, saúde, entre outros. A este prejuízo direto e imediato somam-se a suspensão de contratos, a flexibilização dos pagamentos de prémios, a inevitável redução do número de novas apólices, bem como a não renovação de uma grande parte destas. Os principais analistas mundiais estimam mesmo que esta venha a ser a maior queda de sempre da indústria, superando a crise financeira e as catástrofes naturais anteriores.

Confrontado com um cenário dramático, o setor tem, contudo, sabido desempenhar o seu papel e dar um decisivo contributo para a resposta a esta crise. Desde logo, através da aplicação de moratórias, bem como do ajustamento dos prémios e das coberturas à nova realidade. Um pouco por todo o Mundo, têm sido adotadas um conjunto de medidas extraordinárias, como a concessão de benefícios e compensações adicionais a determinados trabalhadores e negócios, maioritariamente na área hospitalar e da saúde. Em paralelo, várias seguradoras optaram pelo reembolso de apólices onde se regista uma redução do risco e, consequentemente, do número de indemnizações. Todas estas medidas traduzem-se num apoio claro, direto e imediato à tesouraria das famílias e das organizações.

Por último, a indústria seguradora, muitas vezes associada a um conservadorismo e uma certa aversão à modernização, tem sabido adaptar-se à nova realidade e preparar, de forma sustentada, o futuro. Transversalmente, o setor rapidamente renovou o seu modelo de negócio, transferindo para o digital uma significativa parte da sua atividade, e garantindo, desta forma, a capacidade de resposta às necessidades prementes dos segurados, mesmo durante o período de confinamento. Simultaneamente, novas tipologias de seguro foram criadas, em linha com as novas necessidades e realidades das empresas, como o teletrabalho, e outras viram as suas coberturas atualizadas, como é o caso dos seguros de saúde (para inclusão dos testes à Covid-19, bem como da telemedicina). A área da cibersegurança, que mereceu, face às características da atual crise, um significativo impulso e investimento das organizações, é outra das grandes apostas das seguradoras, com vista à criação de soluções que permitam a efetiva proteção das empresas que apostam no digital para garantir a continuidade do seu negócio.

Perante uma crise que não conhece precedentes na história mundial, a solução terá de assentar numa resposta conjunta, transversal a todos os setores de atividade e países, assente em valores como a solidariedade, a resiliência e a inovação. ●

ENTREVISTA SJOERD SMEETS Chief risk officer do grupo Ageas Portugal

Digitalização e proteção cibernética marcará o futuro dos seguros

A era pós Covid-19 nos seguros será marcada pela digitalização, sobretudo na forma como as seguradoras prestam serviços. Outro foco será a proteção cibernética e potenciais coberturas para a interrupção temporária de negócios, afirma Sjoerd Smeets da Ageas Portugal.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

Em termos de cenário macroeconómico para a Europa e em particular para Portugal para 2021, a Ageas identificou uma base e um cenário pessimista da evolução macroeconómica em Portugal, que teve por base previsões das taxas de desemprego – que irão subir até 10%, até ao final do ano, com um ligeiro declínio em 2021 -, e para o PIB – com uma quebra este ano e um ligeiro aumento em 2021. "Esta teve como objetivo apoiar uma reflexão estratégica do impacto da pandemia da covid-19 no nosso negócio: como devemos redefinir as nossas prioridades de negócio para servir os clientes e continuar a ser um player relevante nos seguros, não só em Portugal. Acreditamos que devemos manter o foco no digital, na assistência ao cliente, suporte médico e composição do produto", afirma Sjoerd Smeets, *chief risk officer* do grupo Ageas Portugal.

Questionado sobre o modelo de gestão em situação de crise, o responsável disse que o grupo tem em Portugal um comité de gestão de crise e que é responsável pelos planos desde o aparecimento dos primeiros casos em Portugal. "Criámos vários grupos de trabalho, com foco nos recursos humanos, comunicação, vendas, operações e impactos financeiros". Adiantou que com esta abordagem proactiva "conseguimos ter quase todos os nossos colaboradores, incluindo os centros de atendimento ao cliente, a trabalhar eficientemente a partir de casa. Isto aconteceu de forma quase imediata após a declaração de estado de emergência pelo Governo. Ao nível de negócio, adaptámos os nossos procedimentos de vendas, introduzindo o apoio digital para todos os clientes, tanto em questões mais técnicas como na linha Médis; alargámos as condições de pagamento a clientes com dificuldades financeiras e ampliámos coberturas para fazer face aos desafios desta pandemia". Frisou que "neste período, toda a gestão de topo do Grupo Ageas Portugal foi desafiada a refletir sobre os riscos e oportunidades desta pandemia".

O cibercrime

Questionado sobre o risco crescente de cibercrime neste período disse que "de forma transversal a todos os setores de atividade, em Portugal e em todo o mundo, as pessoas começaram a trabalhar remotamente a partir de suas casas. Como em muitos casos esta mudança foi súbita, nem todas as empresas tiveram tempo de implementar os mecanismos de segurança adequados para os seus colaboradores. Muitos destes nem estavam completamente cientes de todos os riscos cibernéticos. Os cibercriminosos estão a tentar explorar esta vulnerabilidade e o número de ataques de spam, phishing e malware está a aumentar muito (pelo menos em 35%). É crucial que todos estejam bem cientes dos riscos que correm, e que utilizemos a internet de forma mais responsável, com proteção e de forma a reduzir os riscos de ciberataques".

E sobre o futuro dos seguros frisou que na sua maioria, os seguros permanecerão como são hoje, pois cobrem uma necessidade básica – a proteção – seja de propriedade, vida ou saúde. "Algumas alterações podem ser feitas, como um novo foco na proteção cibernética e potenciais coberturas para a interrupção temporária de negócios. No entanto, a maior mudança será na transformação digital. Esta pandemia acelerou esse processo, nomeadamente no setor segurador, especialmente na forma como as seguradoras prestam serviços de vendas, sinistros, reclamações e subscrição. Nas vendas, os canais digitais estão a ganhar relevância, mas também os canais mais tradicionais como os mediadores ou o canal bancário tiveram necessidade de se reinventar e apostar em ferramentas digitais como suporte ao negócio. Ao nível dos sinistros, os clientes não precisam de se deslocar a uma oficina para fazer a peritagem ao veículo em caso de acidente, podem fazê-la na comodidade da sua casa, garagem ou escritório. E nos seguros de saúde, os clientes começaram a utilizar soluções de telemedicina. A Médis é um excelente exemplo, porque o Médico Online tem uma avaliação muito positiva do cliente, de 4,8 em 5".

E sobre solvência, Sjoerd Smeets diz que embora a crise da Covid-19 tenha levado a inevitáveis perdas nos investimentos, "temos uma boa gestão de risco em vigor - a nossa solvência manteve-se forte, em 227% a 30 de junho de 2020, com base no padrão da ASF. O mercado tem uma solvabilidade de 165%, o que significa que o Grupo Ageas Portugal é uma empresa financeiramente muito forte e que está bem posicionada no mercado mesmo na eventualidade de uma segunda vaga da pandemia". Outro tema forte nos seguros é as moratórias e o diferimento do pagamento dos prémios. Refere que "as seguradoras, de forma geral, pretendem proporcionar estabilidade financeira aos seus clientes quando eventos inesperados, como este, acontecem. E, por isso, os seguros têm um papel significativo na sociedade. Nesse sentido, obviamente que concordamos com as medidas do regulador." ●

SJOERD SMEETS
Chief risk officer do grupo Ageas Portugal

FÓRUM

PANDEMIA TROUXE MAIOR VISIBILIDADE AO CIBERCRIME

As pequenas empresas e as famílias ainda estão longe da efetiva valorização dos riscos e das perdas potenciais com o cibercrime. O phishing e as falsas instruções em relações comerciais fraudulentas são algumas dessas manifestações. VÍTOR NORINHA

SUSANA MAYER
Responsável de Marketing de Clientes da Tranquilidade e Generali

"A preocupação com os riscos cibernéticos tem ganho importância nos últimos anos, particularmente entre as empresas de maior dimensão ou ligadas a setores com informação mais sensível ou com exigências de compliance mais forte como serviços financeiros, tecnologia ou saúde, em que o risco de perda, adulteração ou sequestro de dados é crítico para a operação e sobrevivência do negócio por motivos operacionais e de reputação. O que a pandemia trouxe foi uma maior visibilidade para o público em geral com impacto nos pequenos negócios e famílias, devido às notícias nos meios de comunicação e alertas das entidades oficiais. No entanto, e face às limitações financeiras, há pouca capacidade de efetiva valorização dos riscos e perdas potenciais. Assim, a procura proativa pelos clientes por este tipo de soluções é ainda reduzida. Esperamos que esta situação evolua de forma mais rápida no futuro.
Os ataques que impactam mais as famílias ocorrem com tentativas de phishing através de emails que procuram mimetizar comunicações de empresas conhecidas no mercado e que visam, sob essa capa, a recolha de dados das pessoas. Outras situações que surgem são falsas instruções em relações comerciais fraudulentas, como a que tem ocorrido relativamente ao MB Way, que decorrem da baixa literacia financeira e digital dos consumidores.
A Tranquilidade | Generali tem soluções de diagnóstico e resolução de problemas que possam decorrer de ataques para os seus clientes particulares e empresas. Clientes Empresa – em todos os seguros Multirrisco Empresas disponibilizamos a cobertura de prevenção de riscos cibernéticos, com várias funcionalidades como:

- análise de vulnerabilidades do sistema informático
- apoio em caso de ataque informático
- possibilidade de fazer back-up de dados de forma segura

Também disponibilizamos um seguro de Cyber-Risk que pode ser contratado em conjunto com o seguro Multirrisco ou isoladamente. Aos clientes com este seguro, indemnizamos os danos provocados a terceiros, devido a ataque à própria rede informática, assim como despesas de recuperação de dados e limpeza de vírus, permitindo reaver por a situação da empresa antes do ataque, ou ainda outras despesas, incluindo despesas com ransomware, quando legalmente permitido, ou despesas com ações de relações públicas. Clientes particulares – no novo seguro de Casa, recentemente lançado, dispomos de uma cobertura de Proteção Digital com vigilância dos seus dados e apoio, a qualquer hora, em situações como roubo ou uso indevido da identidade.

RICARDO AZEVEDO
Diretor Técnico da Innovarisk

"O mundo de hoje está claramente mais preocupado, tanto a nível das organizações como dos indivíduos na sua esfera privada. As pessoas têm uma percepção cada vez mais clara da forma como a tecnologia influencia a vida de todos e do quão nefasta se pode tornar quando orientada para fins ilícitos, sendo que existe um número cada vez maior de pessoas que já tem um caso para contar e que aconteceu consigo mesmo ou com alguém próximo. Os números referentes a incidentes cibernéticos têm crescido a uma velocidade preocupante, em particular nos últimos meses e na nossa atividade temos notado que cada vez há mais empresas atentas a esta questão, a interessar-se por este tipo de seguros e a adquiri-los. Estes tempos de pandemia acabaram por gerar o terreno propício para a prática de ações de pessoas mal-intencionadas, pelo que as muitas notícias vindas a público sobre o crescimento do número de incidentes e ataques vieram acelerar ainda mais essa consciencialização do risco.
Em pouco tempo, uma quantidade muito maior de pessoas necessitou de usar mais ferramentas digitais e aquelas que já as usavam, aumentaram provavelmente o seu tempo de utilização, pelo que do ponto de vista daqueles interessados em realizar os ataques, houve um aumento gigante do seu mercado potencial. Para além disso, esta maior utilização da tecnologia, ao ser de algum modo precipitada e repentina devido ao confinamento social, aconteceu sem que muitas pessoas e muitos processos estivessem bem preparados em matéria de segurança, ficando à tona uma série de fragilidades que os cibercriminosos puderam aproveitar. Muitas das técnicas utilizadas pelos hackers são as mesmas: phishing, infeção por malware, ataque de negação de serviço, extorsão, SPAM, apenas para citar algumas formas comuns. Mas quando um colaborador responsável por efetuar transferências bancárias se vê subitamente a trabalhar de casa a partir do seu portátil, sem os mesmos sistemas de segurança, com um ecrã de menores dimensões e uma velocidade de ligação mais lenta, com os seus filhos em casa a provocar algumas distrações extra e sem os colegas por perto que o poderiam ajudar a dissipar uma dúvida, provavelmente ficará mais susceptível a cair na ratoeira do phishing e a efetuar uma transferência para as mãos erradas.
O Cyberclear - o nosso seguro de riscos cibernéticos - garante à empresa que o compra uma proteção financeira robusta para o cenário de ocorrência de um incidente cyber ou de violação de dados, quer em relação a perdas próprias que sofra, quer em relação à eventualidade de ter que indemnizar terceiros e assegurar a sua própria defesa jurídica por questões de responsabilidade civil que possam surgir. Para além da tradicional vertente indemnizatória de uma apólice de seguro, o produto permite ainda ao segurado aceder a serviços tecnológicos, jurídicos e de comunicação e relações públicas, que o podem ajudar a ultrapassar mais facilmente o momento de crise que se gera após um ataque ou incidente cibernético."

JORGE TOBIAS
Responsável de Riscos Cibernéticos da Willlis Towers Watson

"A pandemia impôs uma aceleração da transformação digital das organizações antecipando em vários anos aquilo que porventura muitas organizações perspetivavam. No mínimo, a reconversão para trabalho remoto de forma súbita e intensiva veio colocar um grande desafio para as empresas e colaboradores e o que se verificou é que nem sempre terá sido possível introduzir alterações profundas nas formas de trabalho sem colocar a descoberto algum tipo de vulnerabilidades na salvaguarda de informação e/ou de sistemas de IT/OT.
A Covid-19 disponibilizou um campo fértil para esquemas que procuram tirar partido sobretudo da vulnerabilidade dos comportamentos das pessoas. Distribuição de malware e registo de domínios aparentemente genuínos ligados à pandemia procuraram fazer com que os utilizadores pudessem clicar em alguma mensagem / ficheiro com o propósito de capturarem dados de log-in e/ou informação confidencial. Os colaboradores das organizações muitas vezes não resistem ao impulso de clicar em links o que pode de forma involuntária permitir explorar vulnerabilidades do sistema informático das empresas causando sérios problemas financeiros imediatos bem como manchar a reputação das empresas e/ou expor as mesmas a problemas regulatórios severos.
Motivações políticas, religiosas ou outras, estão na base de ataques cibernéticos mas porventura não será um fenómeno que tenha sido exacerbado pelo contexto pandémico. Uma importante exceção será, no entanto, os casos noticiados sobre a tentativa por parte de hackers russos de tentarem aceder a informação sobre o desenvolvimento de vacinas para a Covid-19 no Reino Unido.
Na Willis Towers Watson procuramos trabalhar com os nossos clientes ao nível de dois pilares que, do nosso ponto de vista, se complementam. Por um lado, na análise, avaliação e quantificação dos riscos cibernéticos das organizações auxiliando as empresas a responder a dúvidas muito concretas tais como: de que forma o risco cibernético pode afetar os seus indicadores financeiros (EBITDA, P&L?) ou qual é o Retorno de Investimento inerente às estratégias de mitigação de risco disponíveis? Esta análise é fundamental para ajudar os gestores a perceberem a criticidade destes riscos e assim terem a capacidade de tomar decisões de gestão adequadas ao seu contexto específico.
Numa segunda vertente auxiliamos na definição de planos de gestão de incidentes e na negociação e colocação de seguros específicos destinados a indemnizar as empresas pelas perdas financeiras incorridas na sequência de um incidente que afete os sistemas de IT/OT da organização e/ou que exponham a organização a uma fuga de dados (Data Breach). Nos dias de hoje não faz sentido ter um seguro contra incêndio, como também não faz não ter um seguro que permita à organização fazer face a estes riscos críticos e com uma multiplicidade de impactos tão abrangente."

MANUEL COELHO DIAS
Cyber Risk Specialist da Marsh Portugal

A pandemia reforçou uma tendência que já se verificava de grande sensibilização para o tremendo impacto dos fenómenos cibernéticos, sobretudo na vida das empresas. A grande mudança, fruto da pandemia, terá sido o despertar para a ação, seja na lógica da prevenção e mitigação, seja na perspetiva da transferência do risco, uma vez que muitas organizações se viram exclusivamente dependentes dos canais digitais para comunicação (interna e externa) e para distribuição dos seus produtos e serviços.
A digitalização dos negócios, e da vida humana em geral, é a grande razão pela qual os ataques acontecem e têm um impacto brutal. A partir do momento em que grande parte do valor de uma empresa se encontra digitalizado (sejam segredos de negócio, bases de dados de clientes, contactos de fornecedores, mas também a operação em si e a cadeia logística), os ativos digitais tornam-se uma camada de valor muito assinalável e apetecível aos criminosos. As grandes tipologias de eventos que têm afetado as empresas são os data breaches em que há mera extração das bases de dados, os ransomwares (nos quais pode ou não haver extração das bases de dados hackeadas), o spear phishing e as fraudes por engenharia social. De acordo com a informação coligida pela Marsh, CMS & Wavestone no The Changing Face of Cyber Claims Report, os ransomwares são a ameaça mais frequente na nossa carteira de clientes, mantendo uma tendência de subida muito assinalável nos últimos anos.
Em termos de soluções o primeiro passo é a avaliação profissional dos riscos: a aplicação de um exercício de conhecimento, identificação e avaliação das ameaças e riscos que o negócio enfrenta. A Marsh, por si só na corretagem de seguros, e mais aprofundadamente através das valências da Marsh Analytics, tem feito um grande esforço de quantificação destes riscos; isto é, a tentativa de valorização de um ciberevento na economia de uma determinada organização. Esta quantificação abarca não só as perdas derivadas de um data breach, por exemplo, mas também a dimensão de disrupção do negócio, traduzida na perda de faturação da companhia. Estes exercícios têm por objetivo ajudar a compreender o risco concreto das organizações numa perspetiva mensurável e, no quadro possível, implementar desde logo ações de retificação. Ao nível da cobertura das perdas, a Marsh emprega uma abordagem de assessoria ao cliente, que parte desta mesma avaliação, e identifica no mercado segurador as coberturas mais fiáveis e adequadas, garantindo a melhor posição de cobertura possível.
Este mercado, dos seguros de riscos cibernéticos, tem conhecido grandes evoluções que permitem deixar os clientes muito confortáveis em relação à possibilidade de ocorrência de ataques, mas também de eventos acidentais".

MANUEL MOITA DE DEUS
Direção de Informática e Auditoria da NacionalGest

"Quando analisamos o sector financeiro e a indústria seguradora em particular há algo de fundamental e transversal: a total dependência da base de dados de clientes e a inexistência de produtos físicos em armazém. Para a maioria dos utilizadores não empresariais o Covid 19 não terá afectado o seu relacionamento com o ciberespaço. A maioria dos cibernautas já vê as plataformas na Cloud como uma forma segura para armazenar os ficheiros realmente importantes e desvaloriza quer o hardware quer o software do equipamento, dado que os repõe se necessário. Nas empresas com um SI estruturado, a implementação do teletrabalho afectou sobretudo o Orçamento. Por exemplo, a NacionalGest, no início da Pandemia, já dispunha de todas as ferramentas para um acesso seguro (IPSec) aos seus sistemas centrais. Por isso, a implementação do teletrabalho resumiu-se à aquisição das licenças extra para acesso remoto. Quem não tenha as soluções profissionais adequadas e utilize equipamento misto (família/trabalho) irá continuara ser um alvo fácil para hackers.

Esses ataques manifestam-se, basicamente, de 3 formas:

- Ataques que têm como finalidade a extorsão, já que os dados são encriptados e é exigida uma quantia pela chave de desencriptação;
- Ataques que destroem os dados existentes e que podem causar sérios danos a uma empresa;
- Ataques que clonam os sistemas da vítima para posterior uso desses dados, sem nada destruir e em absoluto "silêncio," e que serão eventualmente os mais perigosos.

Achamos fundamental a existência da garantia de Responsabilidade Civil e, naturalmente, da cobertura que garanta aos clientes as despesas com a recuperação e restauro do sistema afectado. Sendo um seguro que exige uma análise casuística, dependendo do número de servidores, volume de facturação e outros dados que o segurador possa exigir não é possível avançar com custos."

FREDERICO MACIAS
Partner da Deloitte

"Ainda se regista uma preocupação bastante mais acentuada do lado das empresas do que do lado das famílias em particular. Importa salientar, no entanto, que os ataques às empresas também são geralmente mais lucrativos pelo que a incidência é maior neste segmento. Ainda assim os dados familiares não são seguramente de menor importância, pelo que faria todo o sentido que as famílias adotassem posturas mais cautelosas em especial nesta altura em que cada família está frequentemente toda ligada na mesma rede particular. Por outro lado, a pandemia e a necessidade de usar mais ferramentas digitais tem sido um dos estímulos para o aumento dos ataques cibernéticos. Não são só os números que o suportam, mas o facto de ter assistido pessoalmente a várias incidências deste tipo nos últimos tempos. As formas não são novas, o que mudou foi a frequência dos ataques e a falta de awareness e proteção dos utilizadores que passaram a operar remotamente. Salientaria o aumento das atividades de engenharia social, comprometimento de caixas de correio, domínios maliciosos fazendo referência a endereços infetados com malware e também muitos anexos de e-mails contendo malware.

Para muitas organizações, estar nas suas instalações implica a existência de ferramentas de proteção que não existem, de todo, em modo remoto e isso tornou uma parte significativa da sua força de trabalho mais vulnerável a este tipo de ataques.

E, mais do que pensar na cobertura de perdas sugiro, em primeiro lugar, pensar nas medidas que cada organização pode e deve adotar para as evitar. Não existe um "one size fits all" nesta área. Ainda assim e de forma genérica, com as devidas ressalvas, destaco as atividades de formação e de awareness para os riscos que corremos (não se pretende inibir nada nem ninguém, apenas que sejamos conscientes e cautelosos); a existência e aplicação real de politicas de segurança adequadas a esta nova realidade, bem como de programas de privacidade e proteção de dados numa fase em que a confiança que os utilizadores depositam na organização é cada vez maior; utilização de ferramentas que possibilitem uma adequada gestão de identidades digitais e acessos, cada vez mais remotos e diversificados e de planos e exercícios de resposta a incidentes, sendo o tempo e capacidade de resposta fundamentais; adoção de uma gestão de risco de terceiros, entre muitas outras medidas. Estas medidas podem e devem ser utilizadas para reduzir, dentro do possível, o prémio de risco que uma cobertura implica. Quanto mais resiliente for a organização, menor o risco e, em condições iguais, o prémio associado."

PEDRO PINHAL
Director de Sinistros da MDS Portugal

"Sem dúvida que, após o início da pandemia, assistimos a uma maior preocupação das famílias e empresas relativamente ao risco cibernético. De facto, apesar da consciência para os riscos cibernéticos ser, ano após ano, cada vez maior, a atual pandemia elevou este tipo de riscos a um patamar nunca antes visto. E atingiu de forma transversal toda a sociedade, isto é, cidadãos, famílias e organizações, sejam elas de pequena, média ou grande dimensão. Esta maior preocupação tem fortes motivos para se verificar pois, como revelam os mais recentes dados, o número de incidentes em Portugal e no mundo tem assumido proporções nunca antes vistas. Por exemplo, segundo os dados mais recentes do Gabinete de Cibercrime da Procuradoria Geral da República, nos primeiros cinco meses deste ano tinham sido registadas mais 139% de denúncias de crimes cibernéticos do que em todo o ano de 2019!

A necessidade de reduzirmos a exposição ao risco de contágio e combater a propagação do vírus alterou, de um momento para o outro, a forma como trabalhamos, como adquirimos bens e serviços, como estudamos e como comunicamos, tanto a nível pessoal como profissional. E mudou as rotinas diárias de todos - famílias, alunos e empresas -, empurrando-as para um mundo virtual e tornando-as fortemente dependentes de sistemas informáticos, de ferramentas de comunicação digital e de trabalho remoto.

Perante a ameaça do vírus, o foco das organizações centrou-se na proteção da saúde dos seus trabalhadores e em garantir a continuidade do seu negócio e operações, pelo que, tiveram de assumir alguns riscos no que à segurança cibernético diz respeito. Este contexto resultou, por um lado, no aumento exponencial dos possíveis alvos e, por outro, no incremento das vulnerabilidades de segurança cibernética decorrentes da transição/transformação digital muito acelerada e pragmática, por vezes pouco planeada. Este mundo virtual hiperconectado é, precisamente, o oceano onde navegam os piratas informáticos que, de repente, se depararam com a cenário ideal para conduzir as suas atividades criminosas, estando a aproveitá-lo de forma impiedosa e oportunista.

A MDS, enquanto líder em Portugal na consultoria de riscos e seguro, disponibiliza soluções inovadoras e integradas de transferência de risco preparadas para responderem, eficazmente, aos mais variados e complexos eventos cibernéticos. Estas soluções combinam coberturas típicas de seguros com um conjunto vasto e completo de serviços. Entre estes estão diversas garantias de danos e prejuízos sofridos pela própria empresa, nomeadamente: custos com investigação forense; custos incorridos para substituir, restaurar ou recuperar dados; perdas de lucros por interrupção; custos de notificação de violação de dados; gestão de eventos de extorsão e roubo de identidade; danos reputacionais. Incluem ainda a cobertura pela subtração de fundos via transferência eletrónica (crime cibernético); a responsabilidades perante terceiros lesados; e, serviços adicionais focados na prevenção, monitorização, atendimento imediato pós-evento e serviços especializados de informática forense. Em Portugal os custos revelam-se equilibrados tendo em conta a amplitude de coberturas oferecidas e dependem de uma multiplicidade de fatores como, por exemplo, a faturação, o número de empregados/utilizadores, o sector de atividade ou os capitais."

OPINIÃO

A automação e os seguros

EDUARDO ROMANO
Responsável Internacional pelas Alianças de Seguros da everis

A tecnologia está a trazer mudanças em todos os aspetos da nossa vida, e cada vez essas mudanças são mais significativas. Várias organizações de muitos quadrantes da economia estão a definir uma "fasquia" elevada, permitindo interações com os seus clientes, parceiros ou associados de uma forma simplificada, totalmente digital, onde a experiência pela qual o utilizador passa é a principal aposta.

As organizações não deixaram, nem deixarão tão cedo, de prestar os seus serviços através dos seus canais tradicionais como os balcões, o correio eletrónico ou o telefone, mas há uma transição clara para as plataformas digitais muitas vezes pressionadas pelos próprios utilizadores. Torna-se imperioso ter nas organizações uma visão "omnicanal" das interações dos seus clientes e parceiros dado que todas as interações são importantes e não queremos que quem nos contacte tenha de repetir a informação que já transmitiu anteriormente.

Especificamente nos seguros os avanços nestes sistemas como portais ou aplicações de clientes, mediadores ou outros parceiros de negócio têm sido muito rápidos e não há praticamente seguradora que não disponibilize estes sistemas. Há que dizer que há seguradoras no mercado português que investem mais do que outras. As chamadas "diretas", as que procuram estabelecer somente uma relação B2C, têm por natureza este desafio na sua origem e os sistemas digitais são normalmente bastante avançados e completos. Por outro lado, as que apostam numa distribuição B2B ou B2B2C têm bastante desenvolvidos os sistemas de auto-atendimento dos seus parceiros de negócio, mas não deixam de prestar a devida atenção aos portais e aplicações de clientes. É curioso ver que a mediação, que inicialmente receava que estes sistemas pudessem fazer com que as seguradoras retirassem algum protagonismo ao papel do agente de seguros, está agora confiante que tem mais a ganhar do que a perder. Pode focar-se onde claramente importa – no aconselhamento ao cliente e, consequentemente, no crescimento do seu negócio.

No que concerne ao tipo de experiência de utilizador que devem fazer parte destes sistemas temos de pensar que as seguradoras devem procurar a completa autonomia baseada num sistema robusto, fácil, intuitivo, disponível a qualquer momento. Por completa autonomia entende-se que tudo o que possa ser digitalmente executado ou assistido. Uma realidade que tenho vindo a defender e a implementar junto de várias seguradoras, com quem trabalho na empresa que represento. No caso de clientes temos de ter em conta que a frequência de contacto na maioria dos seguros é muito baixa e que muitas vezes o contacto é feito na presença de uma dúvida, um sinistro ou um evento importante na sua vida (mudança de casa, nascimento de um filho, casamento, etc.).

Já no caso de mediadores ou outros parceiros de negócio temos de pensar que a utilização é bastante diferente e orientada para suportar os comuns clientes da seguradora a efetuarem os seus pedidos ou a desenvolver as normais atividades de mediação como a cobrança, a prestação de contas, o cálculo de comissões, etc.

Em qualquer dos casos a adoção destes sistemas não é "natural", ou seja, não é só porque está disponível a melhor aplicação ou portal que os clientes e mediadores os utilizarão. A ativação destes sistemas tem de fazer parte da estratégia de prestação de serviço ao "cliente" (na sua aceção mais lata – sim, porque um mediador é um cliente para a seguradora, talvez até o seu principal cliente!). E para ativar os sistemas é necessário comunicar, comunicar, comunicar, conduzindo e convidando os clientes a experimentarem as plataformas. ●

ENTREVISTA **NUNO LUÍS SAPATEIRO** associado coordenador nas áreas de Banca, Financeiro e Mercado de Capitais da PLMJ

"É forçoso admitir a possibilidade de extensão do regime das moratórias"

A situação pandémica no país e o impacto na economia e no emprego levam Nuno Luís Sapateiro, advogado na PLMJ a admitir a extensão das moratórias nos seguros. Aliás, o regulador espera apenas uma orientação do Governo.

VÍTOR NORINHA
vnorinha@jornaleconomico.pt

Qual o valor global das moratórias públicas de seguros?
Números divulgados pela ASF, entre 13 de maio e 30 de junho, cerca de 3,3 milhões de apólices viram prolongadas em 60 dias as suas coberturas, e procedeu-se à renegociação do pagamento dos prémios em 1,3 milhões de contratos. De qualquer forma, é importante referir que estes números não refletem as moratórias e outras medidas de flexibilização que foram implementadas voluntariamente pelo setor em momento anterior ao diploma legal que estabeleceu o regime da moratória nos seguros. Na realidade, cumpre recordar que o Decreto-Lei n.º 20-F/2020 de 12 de maio foi publicado após o levantamento do estado de emergência e numa altura em que o setor segurador já tinha antecipado muitas das medidas que vieram a ser publicadas no diploma legal e, em muitos casos, os seguradores foram muito para além do que é exigível neste quadro extraordinário.

O que significa o agilizar do enquadramento jurídico para a obtenção de moratórias nos seguros obrigatórios?
Em traços muito gerais, o regime das moratórias públicas de seguros veio permitir que, na ausência de acordo entre a seguradora e o tomador do seguro quanto a um regime mais favorável para o tomador no que respeita ao pagamento do prémio de um seguro obrigatório, a falta de pagamento desse prémio ou fração na data do respetivo vencimento não determine a resolução automática ou não prorrogação do contrato. Nesses casos e somente quando estão em causa seguros obrigatórios, o contrato é automaticamente prorrogado por 60 dias a contar da data do vencimento do prémio ou da fração devida, salvo se o tomador se opuser à prorrogação.

Que impacto é que a medida terá nos rácios das seguradoras?
Diria que mais relevante que o impacto da própria moratória nos rácios das seguradoras, são os efeitos económicos da pandemia e das medidas de contenção associadas. Na realidade, o forte impacto da pandemia nos mercados financeiros tem levado a uma deterioração dos fundos próprios elegíveis para cobrir o requisito de capital de solvência e esse facto já se manifestou na redução do rácio de cobertura do requisito de capital de solvência por comparação com o período homólogo. Essa mesma realidade também se refletiu na redução do nível do requisito de capital mínimo que corresponde ao nível mínimo de fundos próprios abaixo do qual se considera que os tomadores de seguros, segurados e beneficiários ficam expostos a um grau de risco inaceitável. Ainda que o impacto desta crise e, mais concretamente, da moratória só possa ser aferido num prazo mais alargado e esteja muito dependente das carteiras de cada seguradora, é importante sublinhar a mensagem que tem vindo a ser transmitida pelo regulador no sentido de que as entidades supervisionadas continuam a manter uma situação financeira e de capital sólida que reflete uma gestão sustentável e prudente.

> "Admito que a extensão do atual regime excecional e temporário, a confirmar-se, possa determinar a revisão de alguns pressupostos, tendo por base a experiência acumulada e a evolução do enquadramento sócio económico desde maio

A medida foi acompanhada da necessária flexibilização das regras para a indústria por parte do regulador, ou deverão as mesmas regras sofrer algum tipo de ajustamento?
O regime da moratória dos seguros foi acompanhado por um regime excecional de flexibilização dos requisitos de reporte e divulgação de informação baseada no regime Solvência II, de índole contabilística e comportamental por parte das empresas de seguros, o qual esteve devidamente alinhado com as recomendações da Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA). Essa flexibilização no reporte da informação dita normal no período pré-Covid não invalidou que passasse a existir a obrigação de reporte de alguma informação extraordinária por parte das seguradoras de forma a permitir que a ASF possa monitorizar a evolução da situação financeira e alguns aspetos comportamentais no quadro Covid-19.
Entretanto e com o progressivo (ainda que lento) regresso da atividade económica e das operações das entidades supervisionadas, assistimos a uma recente reversão de algumas das medidas de flexibilização dos requisitos regulatórios e de supervisão geralmente aplicáveis à atividade seguradora e a um alargamento da periodicidade do reporte extraordinário de informação diretamente relacionada com o impacto da pandemia no setor segurador. Ainda que este regresso gradual à normalidade no que respeita aos deveres de reporte prudenciais e comportamentais e às ações de supervisão pela ASF tenha por base diretivas da EIOPA e a necessária harmonização do processo de supervisão com os demais estados membros, é inegável que a conjuntura de incerteza que vivemos poderá levar a uma nova alteração súbita das medidas de flexibilização e recomendações aplicáveis.

Tendo em conta a situação pandémica do país e o impacto na economia e no emprego, é previsível uma nova extensão do prazo das moratórias?
O regulador já manifestou estar devidamente preparado para a extensão do regime das moratórias nos seguros caso esse venha a ser o entendimento do Governo e a exemplo do que já aconteceu com a moratória para o crédito. Olhando para a situação pandémica do país e o impacto na economia e no emprego, é forçoso admitir a possibilidade de extensão do regime das moratórias nos seguros. Na realidade, os pressupostos que estiveram na génese da publicação do Decreto-Lei n.º 20-F/2020 de 12 de maio permanecem inalterados e não é expectável que esse quadro se venha a alterar até ao dia 30 de setembro, data em cessa a vigência do regime extraordinário. Se atentarmos, por exemplo, ao regime excecional aplicável em caso de redução significativa ou suspensão da atividade, o mesmo deve permanecer aplicável nos próximos meses uma vez que vai continuar a existir um número considerável de empresas com quebras abruptas e acentuadas de, pelo menos 40% da faturação, que vão precisar de medidas de apoio na gestão da sua carteira de seguros.
Admito que a extensão do atual regime excecional e temporário, a confirmar-se, possa determinar a revisão de alguns pressupostos, tendo por base a experiência acumulada e a evolução do enquadramento sócio económico desde maio. Na realidade, é importante distinguir a implementação do regime excecional vigente num quadro de levantamento gradual das medidas do estado de emergência e de total estagnação da economia para a renovação desse mesmo regime num período pós-confinamento e em que se acentua o regresso da atividade económica. Essa mudança de paradigma é particularmente relevante no que respeita à evolução da sinistralidade em alguns segmentos pelo que se poderá justificar um ajustamento das medidas de flexibilização nos seguros obrigatórios, nomeadamente naqueles que se têm revelado, tradicionalmente, deficitários como é o caso do seguro automóvel e de acidentes de trabalho. ●