Seguros contra riscos cibernéticos e a falácia de financiar o cibercrime

eco.sapo.pt/opiniao/seguros-contra-riscos-ciberneticos-e-a-falacia-de-financiar-o-cibercrime

Bruno Castro, Fundador & CEO da VisionWare, apresenta exemplos recentes e insiste que pagar resgates a cibercriminosos só estimula a chantagem.

A dependência tecnológica do tecido empresarial, torna inevitável e cada vez mais preocupante a crescente exposição a ciberameaças. Ciberataques como *phishing* e *ransomware* tornaram-se tão comuns que, para muitas empresas, não é mais uma questão de "se" um ciberataque ocorrerá, mas sim, "quando" irá ocorrer – e, Portugal não é exceção. De acordo com dados recentes divulgados pela Check Point Software, **Portugal está no top três dos países europeus que mais ciberataques sofreu só no terceiro semestre de 2024, registando um total de 2.061 ciberataques.**

Perante este cenário são já milhares as empresas, pequenas, médias e grandes que enfrentaram prejuízos financeiros massivos. Apesar de, as medidas de proteção e defesa cibernética serem imprescindíveis, não são, nem nunca serão, infalíveis. Mesmo quando as medidas de proteção tecnológicas funcionam, os números revelam-nos que, **grande parte dos incidentes ainda ocorrem devido a erro humano –** um fator que é difícil de contornar apenas por recurso a tecnologia. Por este motivo, uma das maneiras pelas quais as organizações tentam mitigar o risco e o impacto dos ciberataques é adquirindo um seguro contra riscos cibernéticos, que cubra os custos e danos associados a um incidente de cibersegurança. São muitas as empresas a reconhecer esta necessidade e, por tendência natural do mercado, **estou convicto de que a procura por esta tipologia de seguro irá sofrer um incremento exponencial,** nomeadamente, em mercados mais expostos ao risco cibernético. **Entre aquelas organizações que sofreram um incidente de *ransomware*, revela a Proof Point, que 96% agora detém um seguro contra riscos cibernéticos.**

Da parte das seguradoras, o que verificamos é que ainda é uma zona algo cinzenta, em particular, no que diz respeito à avaliação de risco aplicada e na apresentação clara e objetiva ao mercado de como funciona e se ativa efetivamente um seguro de risco cibernético, quando necessário. Diria que não é simples transpor o modelo aplicado pelas seguradoras em seguros convencionais, como são os exemplos de um seguro de vida ou seguro automóvel, já que, **na realidade de um seguro cibernético, as variáveis são menos objetivas e muito menos maduras.** Será também um desafio para as seguradoras conseguir estruturar um modelo simples e objetivo, que permita apresentar ao mercado as mais-valias inequívocas de avançar com um seguro deste tipo, e que, quando necessário, também seja fácil e célere de concretizar o respetivo pagamento de prémio.

As seguradoras europeias poderão olhar para as tendências americanas como um exemplo, quer nos casos de sucesso, quer também em lições aprendidas de modo a evitar futuros erros. Veja-se o caso recente, divulgado no *Financial Time*s, através de um alerta de Anne Neuberger, Deputy National Security Advisor for Cyber and Emerging Technologies da Casa Branca, direcionada às seguradoras americanas, invocando que, **estas devem parar de incentivar o pagamento de resgates de ciberataques –** algo que nós, na VisionWare, temos vindo continuamente a desaconselhar**,** quer publicamente, quer junto das vítimas de ciberataques onde estamos envolvidos. Pagar um resgate a um cibercriminoso, significa automaticamente, financiar o cibercrime e, como tal, é necessário ter em atenção quando somos orientados a fazê-lo.

Ainda, de acordo com dados divulgados pela Proof Point, a **larga maioria das seguradoras (91%), no ano 2023, facilitou pagamentos de resgates de incidentes específicos de *ransomware*,** uma percentagem bem acima dos 82% registados no ano anterior. Contudo, globalmente, a taxa de pagamento para invasores de *ransomware* baixou de 64% para 54%. **O número de inquiridos da Proof Point que recuperaram o acesso aos seus dados, após o pagamento de resgate também diminuiu,** o que pode ser uma explicação para a queda nestes pagamentos de resgate. Outra possível razão, é que **as organizações estão a tornar-se elas próprias cada vez mais conscientes das desvantagens e riscos de pagar resgates,** pelo facto de esses, encorajarem a ocorrência de mais ciberataques, financiar atividades criminosas ou receber dados comprometidos e/ou incompletos.

Ainda, olhando para as tendências das seguradoras americanas, o que se verifica é que, apesar destas oferecerem cobertura a ataques *ransomware*, **muitas têm tornado os critérios de adesão mais rigorosos, de forma a também se salvaguardar de elevados custos de cobertura.** Quando se verificam falham graves de cibersegurança por parte de negligência das empresas, será expectável que haja limites nas indemnizações e ativações de seguros para as empresas.

Nesta linha orientadora, e devido às variáveis menos objetivas e maduras subjacentes a um seguro contra riscos cibernéticos, será crítico para as seguradoras portuguesas trabalharem em cooperação com as empresas de cibersegurança, de forma **a chegar a um modelo de negócio que salvaguarde e proteja quer as empresas,** quer as seguradoras e, em simultâneo, que clarifique quais as exigências e requisitos expectáveis para as organizações que queiram ativar este tipo de seguro.