Mais vale (um bom) seguro contra ciberataques na mão do que milhões a voar

digitalinside.pt/mais-vale-um-seguro-contra-ciberataques-na-mao-do-que-milhoes-a-voar

A crescente dependência do tecido empresarial em relação à tecnologia e ao mundo digital, torna inevitável 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 "quando" – e, Portugal não é exceção. De acordo com dados recentes divulgados pela Checkpoint, Portugal está no Top 3 de países europeus que mais ciberataques sofreu só no terceiro semestre de 2024 – 2.061 ciberataques. Perante este cenário, surgem novas opções para as empresas como é o caso de seguros contra ciberataques, que pretendem cobrir custos relacionados com ameaças e impacto cibernético, decorrente de cibercrime, que as empresas não conseguem controlar na sua totalidade.

Muitas organizações ainda hesitam, e subestimam a gravidade das consequências de um ciberataque, mas a verdade é que, atualmente, torna-se difícil ignorar os números alarmantes de incidentes de segurança por todo o mundo. Milhares de empresas, pequenas, médias e grandes entidades já enfrentaram prejuízos financeiros massivos. Ainda assim, os ciberataques não afetam apenas o balanço financeiro de uma empresa – podem destruir a confiança dos clientes, minar a reputação, paralisar operações e, em alguns casos, pode levar a processos judiciais caros e desgastantes. Se olharmos para o mercado, é evidente que, a prevenção contra danos potencialmente catastróficos já está enraizada, mas tal como temos seguros contra incidentes de natureza física, temos de começar a pensar que os danos catastróficos no ciberespaço também trazem consequências graves, acabando por afetar o domínio não virtual de uma forma tão ou mais violenta. A questão é, porque é que esse mesmo raciocínio não é amplamente aplicado à salvaguarda da sua proteção digital?

Apesar de as medidas de proteção e defesa cibernética serem imprescindíveis, não são, nem serão, infalíveis. A comunidade cibercriminosa está constantemente a melhorar as suas técnicas, sendo cada vez mais criativos, sofisticados e eficazes. E 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 meio de tecnologia de proteção e defesa. Por este motivo, um seguro contra ciberataques torna-se relevante para a estratégia de segurança de qualquer empresa face à sua própria gestão de risco, mais especificamente na iminência de um ciberataque violento. Esta tipologia de seguro, além de cobrir prejuízos decorrentes de um ciberataque, poderá também incluir, recursos para lidar com as consequências legais e regulatórias, cada vez mais exigentes nos dias de hoje.

Felizmente, são já muitas as empresas a reconhecer esta necessidade e, por tendência natural do mercado, estou convicto que a procura por esta tipologia de seguro tenderá a crescer de forma exponencial, em mercados mais expostos ao risco cibernético. Da parte

das seguradoras, o que verificamos é que, esta é ainda uma zona algo cinzenta, nomeadamente, na avaliação de risco aplicada, e na apresentação clara e objetiva ao mercado de como funciona um seguro de risco cibernético quando necessário. Diria que não é simples transpor o modelo aplicado pelas seguradoras em seguros convencionais, como um seguro de vida ou automóvel, para a realidade de um seguro cibernético onde as variáveis são menos objetivas e muito menos maduras. Será também um desafio para as seguradoras conseguir criar um modelo simples, que permita apresentar ao mercado as mais-valias de efetivar um seguro destes, e que, quando necessário, também seja fácil e célere de concretizar o respetivo pagamento de prémio.

Dito isto, também é importante destacar que o seguro não substitui nem cobre uma abordagem de governance de segurança adequada, aliás, terá de ter precisamente isso em conta no decorrer da quantificação do risco da empresa para a aplicabilidade (ou não) do próprio seguro. A existência de políticas de cibersegurança, auditorias regulares de avaliação do nível de risco, medidas de proteção e defesa, como por exemplo, as que incluem um SOC (Security Operations Center) ativo, terão de ser, para além de uma estrutura operacional de um modelo de governação de segurança, também as variáveis objetivas onde o seguro de risco cibernético deverá assentar na sua avaliação de risco. Optar por um seguro contra ciberataques deve ser parte de uma estratégia de segurança mais ampla da gestão de topo, envolvendo não apenas tecnologia, mas também uma cultura organizacional que valorize a segurança da informação a todos os níveis.

Neste sentido, e devido às variáveis menos objetivas e maduras subjacentes a um seguro de riscos cibernéticos, será importante para as seguradoras europeias trabalharem em conjunto com as empresas de cibersegurança, de forma a chegar a um modelo de negócio que salvaguarde quer as empresas, quer as seguradoras e, ao mesmo tempo, que clarifique quais as exigências expectáveis para as empresas que queiram ter um seguro deste tipo ativo.

Em última análise, um seguro de risco cibernético deve ser encarado como uma parte essencial, ainda que, complementar, no modelo de proteção empresarial do século XXI. Para as empresas, ignorar esta realidade é um risco que ninguém se pode dar ao luxo de correr e, para as seguradoras, o trabalho futuro passará por compreender como tornar estes seguros capazes de atender às necessidades reais das empresas, sobretudo das PME, grande fatia do tecido empresarial português. Fica lançado o desafio para discussão futura.

Bruno Castro é Fundador & CEO da VisionWare. Especialista em Cibersegurança e Investigação Forense