

Número de incidentes no Brasil cresceu 48% em 2014 e empresas globais precisam se adaptar para novos modelos de crimes

A resseguradora Allianz Global Corporate & Specialty (AGCS) analisa em seu novo relatório - **Um Guia para os Riscos Cibernéticos: Administrando o Impacto da Interconectividade Crescente** - as últimas tendências em risco cibernético e ameaças emergentes pelo mundo. De acordo com o guia, riscos cibernéticos são o tipo de ameaça que mais cresce, custando aproximadamente 445 bilhões de dólares por ano, dos quais metade estão relacionados às 10 maiores economias do planeta.

No Brasil, os ataques cibernéticos aumentaram 48% em 2014, segundo o estudo “Managing cyber risks in an interconnected world” da PWC. O estudo mostra ainda que o número de incidentes cibernéticos detectados subiu para 42,8 milhões em relação a 2013 (o equivalente a 117.39 novos ataques todos os dias).

“Há 15 anos, os ataques cibernéticos eram rudimentares e ações típicas de ativistas hackers, mas com a interconectividade crescente, a globalização e a comercialização dos crimes cibernéticos houve um aumento tanto na frequência como na severidade dos ataques,” explica o CEO da AGCS Chris Fischer Hirs. “A AGCS enxerga uma demanda crescente por esses serviços e nós estamos comprometidos a trabalhar com nossos clientes para entender e responder melhor ao aumento da exposição aos riscos cibernéticos.”

Políticas de regulação rígidas e novas ameaças cibernéticas

O crescimento da conscientização sobre a exposição no meio digital assim como mudanças regulatórias irão acelerar o crescimento do seguro contra riscos cibernéticos. Com pouco mais de 10% das companhias a oferecerem atualmente apólices específicas para esse tipo de risco, a AGCS prevê que os prêmios para os seguros contra riscos cibernéticos passarão de 2 para 20 bilhões anuais na próxima década, registrando uma taxa de crescimento anual de mais de 20%.

Anteriormente, a atenção estava voltada aos vazamentos de dados, mas a nova geração de riscos cibernéticos é muito mais complexa: as ameaças futuras serão relacionadas ao roubo de propriedade intelectual, ciberextorsão e ao impacto da interrupção das operações ou falhas técnicas causadas por um ciberataque, riscos que normalmente são subestimados.

Conectividade cria riscos

O aumento da interconectividade nos dispositivos do dia-a-dia e da confiança na tecnologia tanto no âmbito pessoal quanto no corporativo resultará em futuras vulnerabilidades. Algumas estimativas sugerem que um trilhão de dispositivos podem estar conectados até 2020, enquanto ainda preveem que mais de 50 bilhões de máquinas poderão trocar dados diariamente.

Eventos catastróficos

Com o grande número de ocorrências de vazamento de dados, a probabilidade de uma perda catastrófica tem aumentado. Como será essa perda, entretanto, é difícil de prever. Os cenários incluem ataques à infraestrutura central da internet e até mesmo a empresas de energia ou utilidade pública, podendo resultar na escassez de serviços e na possibilidade de perdas de vidas no futuro.

Cobertura autônoma

A Allianz prevê que o foco do seguro contra riscos cibernéticos precisa evoluir para prover uma cobertura mais abrangente e completa ao incluir interrupções de operações e estreitar os espaços entre a cobertura e políticas para regulação da tecnologia.

Respondendo ao risco cibernético

O relatório da AGCS destaca os passos que as companhias podem tomar para se proteger contra riscos cibernéticos. O seguro é apenas parte da solução, mas uma abordagem de gerenciamento de riscos abrangente é a fundação para uma boa defesa cibernética. “Uma vez que o seguro contra riscos cibernéticos tenha sido adquirido, isso não significa que a segurança de TI possa ser ignorada. Os aspectos tecnológicos, operacionais e de seguro estão de mãos dadas”, explica Jens Krickhahn, especialista em cibernética e fidelidade da AGCS no Centro e Leste Europeu. A AGCS recomenda uma abordagem integrada onde diferentes especialistas da empresa colaborem para compartilhar conhecimento.

[Clique aqui para ler o relatório na íntegra](#)

Fonte: S2PUBLICOM, em 09.09.2015.