Swiss Re

As perguntas certas são o segredo

Uma análise do risco cibernético nas empresas de pequeno e médio porte

A digitalização da economia e da sociedade proporciona diversas vantagens. Vivemos em um mundo onde praticamente todos têm um smartphone, compram produtos pela Internet e usam serviços de streaming multimídia. Sob a bandeira "Indústria 4.0", as empresas estão se beneficiando da rapidez e do aumento de eficiência prometidos pela digitalização dos processos operacionais. Enquanto isso, estações de trabalho no PC funcionais e conexões rápidas à Internet também se tornaram essenciais para as atividades de negócios das empresas de pequeno e médio porte. Porém, a digitalização e a interconectividade crescentes também estão criando um alto grau de dependência de sistemas de TI funcionais e seguros, bem como a necessidade de pessoal bem qualificado.

Há vários anos, falhas de sistemas e ataques de hackers tem provocado cada vez mais casos de interrupção dos negócios, e o vazamento de dados também tem sido oneroso para empresas de todos os portes. No relatório anual "Barômetro de Risco" de 2018, da Allianz, a interrupção dos negócios e os incidentes cibernéticos são considerados como os dois maiores riscos para as empresas. Na maioria dos países ainda não há a obrigatoriedade de informar os incidentes cibernéticos, entretanto, podemos estimar as perdas anuais em todo o mundo em torno de US$ 400 bilhões.

As empresas de pequeno e médio porte estão mais cientes dos riscos cibernéticos e de seus impactos negativos sobre as operações comerciais normais. Em grande parte, isso foi impulsionado pelo surgimento de regulamentos de proteção de dados em diversos países o que, por sua vez, tem levado as pequenas e médias empresas (PME) a se interessarem pela análise de seus riscos de TI, protegendo-se e transferindo parte de seus riscos cibernéticos para as seguradoras.

Muitas seguradoras de ramos elementares e de responsabilidade civil têm reconhecido esse risco e estão oferecendo seguros cibernéticos para proteger as empresas dos custos elevados de incidentes nessa área. Os itens mais populares de cobertura para o próprio segurado incluem interrupção dos negócios, recuperação de dados e extorsão cibernética. Para perdas de terceiros existe cobertura para pedidos de indenização relativo a eventual perda de dados pessoais, multas contratuais de PCI (sistema de conexão para transmissão de sinais utilizado pelo setor de cartões) e responsabilidade de rede/multimídia. Um papel importante também é desempenhado pelo "componente de serviço" oferecido pelas seguradoras, como análises de segurança, medidas preventivas, treinamento e mediação de especialistas em casos de sinistros.

Para calcular os prêmios adequados para a cobertura cibernética, as seguradoras precisam compreender os riscos cibernéticos de seus clientes. Os analistas de risco cibernético auxiliam os subscritores no processo de tomada de decisões, analisando a exposição ao risco cibernético e a adequação das medidas de proteção. Para tanto, eles precisam de amplas informações dos possíveis segurados, na forma de questionários preenchidos, apoiando a documentação e a discussão de riscos.
É necessário esclarecer a abordagem geral do proponente à gestão do risco de TI e entender os complexos sistemas, redes e organização de segurança envolvidos. Frequentemente, esse tipo de análise se assemelha a uma auditoria externa de segurança cibernética, que pode durar dias ou até mesmo semanas, o que significa que ela só pode ser usada para avaliar riscos vultuosos.

No caso das PMEs, em virtude do baixo valor dos seguros e prêmios envolvidos, as seguradoras não têm condições de arcar com as custosas e demoradas análises de riscos cibernéticos. Consequentemente, a maioria das seguradoras trabalha atualmente com questionários convencionais de risco, parte deles ainda impressos, mas que cada vez mais podem ser preenchidos ***online.*** Por exemplo, em sua versão básica, o questionário modelo da Associação das Seguradoras Alemãs apresenta 10 perguntas, com outras que podem ser acrescentadas dependendo do potencial de risco. Por exemplo, empresas com faturamento anual entre €5 e €10 milhões e que processam dados reservados devem responder a 35 perguntas. Dependendo do valor segurado e dos elementos de cobertura considerados, algumas seguradoras reduzem seus questionários sobre riscos cibernéticos para menos de cinco perguntas e fazem referência aos requisitos adicionais de segurança de TI estipulados em suas condições gerais de seguros.

Em geral, os questionários de risco abrangem duas áreas distintas: exposição ao risco e qualidade do risco. Sobre a exposição ao risco é importante para as seguradoras saberem o tamanho exato e o faturamento anual da empresa, bem como o setor em que ela atua. Outras questões essenciais envolvem o volume de dados pessoais armazenados e processados pela empresa e sua dependência do funcionamento dos sistemas de TI.

Cinco critérios são essenciais para entender até que ponto uma empresa se protege contra os ataques e o impacto dos incidentes de segurança de TI: identificação das informações e dos recursos que precisam ser protegidos, sua proteção adequada, reconhecimento de ataques e incidentes, reação adequada a eles e a recuperação ordenada dos sistemas, processos e dados de TI após um incidente.

No caso das PMEs, perguntas relativas às medidas básicas essenciais de segurança são de suma importância:

- Existe um sistema de gerenciamento de acessos, bem como treinamentos regulares em segurança de TI para os funcionários?
- O software é atualizado em intervalos regulares e há sistemas antigos em uso?
- Os computadores, laptops e redes contam com segurança adequada e ficam separados uns dos outros?
- As cópias de segurança são feitas regularmente?

É relativamente fácil para as seguradoras adotarem questionários cibernéticos para as PMEs e, em geral, seu preenchimento não exige muito tempo. Com questionários virtuais, as respostas podem ser avaliadas e as ofertas preparadas rapidamente. Contudo, os resultados da pesquisa indicam que os questionários de seguros são respondidos pelos próprios diretores administrativos das PMEs, o que representa um certo perigo, já que nem sempre eles estão familiarizados com esse conjunto de problemas relativamente novos, altamente complexos e em rápida mutação. Frequentemente eles subestimam a situação das ameaças à sua empresa e superestimam seu nível de segurança de TI.

Outra possível abordagem para a avaliação de riscos é o uso de uma análise de "fora para dentro". Ela envolve a avaliação externa do nível de segurança de uma empresa, usando dados e varreduras disponíveis publicamente, mas sem o envolvimento ativo da empresa analisada. Nesse processo, são coletados dados de empresas vulneráveis e de sistemas afetados, configurações não seguras e vazamento de dados. Além dos fatores tecnológicos, fatores econômicos e comportamentais obtidos em diversas fontes também são levados em consideração para determinar um perfil de risco abrangente.

Tais análises espelham a abordagem dos autores de ataques, cujo primeiro passo é coletar informações sobre as vítimas vulneráveis. Mas, ao contrário de um ataque, os sistemas de uma empresa são apenas objeto de uma varredura, sem serem efetivamente penetrados. Os provedores desses serviços incluem a BitSight, Cyence, Security Scorecard e uma série de ***startups.*** Esse tipo de avaliação tem diversas

vantagens: é realizada de forma automatizada em intervalos regulares, executa análises objetivas e comparáveis, e também pode levar rapidamente em consideração novas falhas e fontes de dados. Contudo, como essas varreduras não examinam o funcionamento interno da empresa, permitem apenas uma avaliação externa e, portanto, limitada da vulnerabilidade técnica. Ao avaliar uma PME, essa abordagem pode ser limitada pela tendência dessas empresas de, dependendo de seu setor, terem uma presença digital pequena.

No futuro, é provável que abordagens combinadas ofereçam o melhor potencial para a análise do risco cibernético das PMEs. Um exemplo seria uma varredura automatizada de fora para dentro, executada paralelamente ao preenchimento de um questionário virtual e verificação das páginas na web indicadas pela empresa. Isso permite uma análise direta das informações sobre gerenciamento de correções e configurações seguras. As ameaças cibernéticas estão em constante evolução, de forma que tomar como base o cenário de risco no momento da subscrição não é suficiente. Ao invés disso, seguradoras e segurados precisam que sua carteira e exposição em TI sejam constantemente mensuradas e calculadas. Uma opção seria a integração dos resultados da varredura de software ou hardware usada na rede interna da PME para examinar os sistemas, configurações e falhas de segurança.

A indústria de seguros desenvolveu abordagens iniciais e procedimentos estruturados para a análise do risco cibernético das PMEs. O cenário de mudança constante das ameaças, novas formas de análise em casos de sinistro cibernético e o progresso tecnológico terão impacto sobre o desenvolvimento de métodos de análise de risco. As seguradoras de riscos cibernéticos devem determinar seus prêmios com base nos resultados da análise objetiva dos riscos e nas medidas de proteção empregadas pelos segurados. Dessa forma, o mercado segurador pode desempenhar um papel importante para estimular a maturidade cibernética de uma economia como um todo, bem como ajudar a ampliar a resiliência cibernética de cada empresa.

Autor
Thomas Schnitzer – Senior Cyber Risk Analyst – Swiss Re

Disclaimer

Swiss Reinsurance Company Ltd
Mythenquai 50/60
P.O. Box
8022 Zurich
Switzerland

Telephone +41 43 285 2121
Fax +41 43 285 2999
www.swissre.com

7/25/18