Apólice ideal depende de necessidades exclusivas de cada organização

À medida que o cenário digital evolui, o seguro cibernético vem se tornando fundamental para que empresas de todos os portes protejam seus ativos digitais e mantenham a resiliência operacional. De acordo com a Superintendência de Seguros Privados (SUSEP), autarquia vinculada ao Ministério da Economia, responsável pelo controle e fiscalização do setor, no primeiro semestre de 2023 os seguros cibernéticos no Brasil registraram R 98,12 milhões no acumulado de prêmios, alta de 27,2% em relação ao mesmo período do ano anterior.

As apólices de seguro cibernético geralmente se enquadram em duas categorias principais: cobertura primária e cobertura de terceiros.

O seguro cibernético primário trata das perdas financeiras sofridas pelo segurado como resultado de um evento cibernético, seja um ataque ou violação de sua rede ou sistema. Basicamente, engloba fraude/roubo, perda de dados e trabalho de restauração, interrupção de negócios, ameaças de extorsão cibernética, investigação forense, reparo de imagem da empresa e notificações ao cliente. A cobertura dessa categoria geralmente vem acompanhada de seguro contra erros e omissões.

Já o seguro cibernético de terceiros oferece cobertura para quaisquer ações de responsabilidade contra o segurado após um evento. Essa responsabilidade pode ser reivindicada por clientes, fornecedores, reguladores ou qualquer parte que procure reparação financeira da empresa devido a um incidente cibernético. Sua cobertura geralmente inclui honorários advocatícios, custos de liquidação, pagamento de danos judiciais, custos relacionados à resposta a consultas regulatórias, multas e penalidades governamentais.

"A escolha da apólice de seguro cibernético correta pode ser uma tarefa desafiadora, pois o setor está em constante evolução, e as seguradoras atualizam frequentemente suas ofertas", explica Germán Patiño, vice-presidente de vendas para a América Latina da **Lumu Technologies**, empresa de cibersegurança criadora do modelo Continuous Compromise Assessment™. O executivo também lembra que nenhuma apólice é universal, e que a melhor escolha depende de necessidades exclusivas de cada organização.

A seguir, Patiño lista as principais orientações que os CISOs devem considerar na escolha de um seguro cibernético.

1. **Requisitos de controle**: é fundamental desenvolver planos de implementação para controles rigorosos;
2. **Limites do seguro**: o CISO deve ter em mente as restrições com base em setores específicos ou limites de receita;
3. **Eventos generalizados**: é preciso estar ciente das limitações de cobertura para eventos generalizados;
4. **Cosseguro para ransomware**: é importante para o líder de cibersegurança entender os requisitos de cosseguro para esse tipo de ataque;
5. **Exposições de vulnerabilidades críticas**: vulnerabilidades devem ser tratadas imediatamente, pois atrasos podem resultar na negação da cobertura;
6. **Exclusões de cobertura de hardware e software antigos**: eventuais atrasos na cadeia de suprimentos devem ser planejados, a fim de priorizar as atualizações de hardware e software em fim de vida útil;
7. **Funcionários remotos**: recomenda-se buscar orientação jurídica sobre o monitoramento permitido de funcionários remotos;
8. **Zero day**: deve-se estar atento às exclusões de cobertura relacionadas a vulnerabilidades de zero day e, se necessário, explorar políticas alternativas;
9. **Aumento no prêmio do seguro**: os controles devem ser aproveitados para se posicionar na categoria de prêmio ideal em meio ao aumento dos custos.

Todavia, ter uma apólice não elimina riscos nem garante imunidade à organização, pois violações recorrentes e alto índice de perdas podem inviabilizar o seguro. Também é importante que se observe quais itens são excluídos de cobertura, tais como processos de segurança ineficazes, violações anteriores, falha humana, ataques internos e vulnerabilidades pré-existentes.

"Entender as complexidades do seguro cibernético e seus principais componentes é crucial para os líderes de cibersegurança tomarem decisões informadas e adaptadas ao perfil de suas organizações. Também é essencial trabalhar ativamente para mitigar os riscos após a assinatura do contrato e manter-se informado sobre mudanças nas apólices que possam afetar a estratégia de segurança. Não fazer isso pode transformar a apólice de uma medida de proteção em um passivo financeiro para a seguradora", conclui Patiño.

Sobre a Lumu Technologies

Com sede em Miami, Flórida, a Lumu é uma empresa de cibersegurança focada em ajudar organizações empresariais a identificar ameaças e isolar instâncias confirmadas de comprometimento. Ao implementar os princípios do Continuous Compromise Assessment™, a Lumu criou uma poderosa solução de feedback e autoaprendizagem que ajuda as equipes de segurança a acelerar a detecção de comprometimentos confirmados, obter visibilidade em tempo real em sua infraestrutura e fechar a lacuna na detecção de falhas de segurança de meses para minutos. Saiba mais sobre como a Lumu identifica os pontos de comprometimento da rede em wwwlumuio.

Fonte: Pimenta Comunicação, em 25.03.2024