Por Roberto Regente Jr., vice-presidente da OpenText para América Latina e Caribe

À medida que a frequência e o escopo dos ataques cibernéticos aumentam, também aumenta o custo do seguro cibernético. Pior ainda, algumas empresas estão solicitando cobertura e sendo rejeitadas porque os subscritores de seguros cibernéticos concluíram que essas companhias representam um coeficiente de risco alto porque não possuem mecanismos e programas suficientes para se proteger contra os ataques.

O seguro cibernético não é diferente de qualquer outro seguro, pois seu custo depende do risco associado à cobertura. O aumento drástico no risco de incidentes cibernéticos é o principal impulsionador da ascensão do mercado global de seguros de segurança cibernética, que deve crescer de US$ 9,29 bilhões em 2021 para US$ 38,7 bilhões até 2030.

Assim como os provedores de seguros de automóveis oferecem um desconto para um registro de direção segura e os provedores de seguros residenciais oferecem um desconto para a implementação de um sistema de segurança residencial, os provedores de seguros cibernéticos são mais propensos a oferecer não apenas cobertura de seguro cibernético quando sua organização demonstra um programa abrangente de segurança cibernética, mas também estarão mais propensos a oferecer taxas mais baixas para essa cobertura.

Como a organização pode maximizar sua capacidade de obter seguro cibernético enquanto mantém os custos contidos na medida do possível? Aqui estão dez passos para combater o alto custo do seguro cibernético:

1. **Implementar a autenticação multi-fator (MFA)**: a implementação da proteção MFA em todos os aplicativos que a suportam pode ajudar a proteger informações confidenciais, principalmente no que diz respeito a sistemas de dados valiosos e de missão crítica, tornando as credenciais roubadas inúteis sem o dispositivo de autenticação.

2. **Aplicar os Princípios de Menor Privilégio (Principles of Least Privilege - POLP)**: atualize a segurança de sua organização controlando rigidamente os direitos de acesso a seus sistemas operacionais e aplicativos. Crie contas de usuário dedicadas com privilégios limitados adaptados para tarefas específicas, para que tudo corra bem – e com segurança! – quanto possível e garanta que seus provedores de nuvem façam o mesmo.

3. **Aplicar atualizações e patches prontamente**: manter o software e os sistemas operacionais atualizados com os patches de segurança mais recentes é uma forma essencial de prevenir possíveis ameaças. Por isso é importante monitorar quando os provedores emitem patches que eliminam vulnerabilidades e aplicá-los prontamente (antes que os hackers, que também os monitoram, possam aproveitá-los).

4. **Realizar testes de backup e recuperação**: para garantir que você esteja preparado para o pior, estabeleça backups regulares e testes de recuperação de seus dados principais. Isso fornece um controle inestimável para limitar as interrupções causadas por atividades maliciosas, como ataques de ransomware.

5. **Endpoint Detection and Response (EDR)**: mantenha seus dispositivos conectados seguros com uma solução de segurança EDR. Essa tecnologia coleta ativamente dados sobre sistemas conectados, realiza análises baseadas em regras para detectar atividades maliciosas e, em seguida, gera respostas automatizadas projetadas para proteger contra ameaças cibernéticas.

6. **Filtros de segurança de e-mail**: manter seus filtros de spam e malware atualizados é uma maneira eficaz de se proteger contra tentativas de phishing, reduzindo significativamente o risco.

7. **Implementar uma solução de gerenciamento de dispositivos móveis (MDM)**: a

implementação de soluções MDM pode ser uma maneira vital de ajudar a manter os dispositivos móveis seguros. Especialmente no contexto de um ambiente BYOD (Bring your own device - Traga seu próprio aparelho), em que os dados pessoais e comerciais são misturados em um único dispositivo, essas soluções fornecem às organizações proteção valiosa contra riscos potenciais.

8. **Minimização, criptografia e monitoramento de dados**: manter a privacidade dos dados é essencial em nosso mundo cibernético. Os dados devem ser classificados, gerenciados e protegidos para reduzir o risco de violação de dados e oferecer suporte à minimização de dados. A eliminação regular de dados redundantes, obsoletos ou triviais (ROT) ajuda a remover dados potencialmente confidenciais da exposição a hackers. A criptografia de dados confidenciais em repouso protege esses dados, mesmo que sejam acessados por ameaças internas ou externas, e o monitoramento da atividade nesses dados confidenciais permite que sua organização reaja rapidamente para encerrar as ameaças antes que elas possam causar algum dano.

9. **Manter a documentação de políticas e procedimentos em dia**: manter as políticas e os procedimentos relacionados à tecnologia, como credenciais e requisitos de senha, atualizados ajuda a garantir a segurança dos dados da sua empresa. A implementação das melhores práticas de segurança é essencial para proteger contra possíveis ameaças cibernéticas.

10. **Treinamento cibernético rigoroso e recorrente**: para garantir que todos os funcionários estejam atualizados sobre os protocolos de segurança mais recentes, devem ser fornecidos intervalos regulares de treinamento abrangente e atualizações. Além disso, o treinamento pontual pode ser realizado para combater os riscos recém-identificados à medida que eles surgem.

Fonte: Vianews, em 29.03.2023