FOTOS: ISTOCK

PARTES RELACIONADAS, UM RISCO ESCONDIDO

Por**: WILSON LAURIA**

No cenário atual de ameaças digitais, um dos vetores de ataque mais comuns consiste na exploração, pelos agentes maliciosos, das fragilidades cibernéticas nas Terceiras Partes Relacionadas (e.g., provedores de suprimentos e serviços). Para o setor automotivo – um segmento econômico que depende de uma extensa e diversificada supply chain – esse fator representa um grave risco sistêmico que, por vezes, passa despercebido.

Recentemente, o incidente da CDK Global – um importante provedor de Dealer Management System (DMS) – impactou a operação de mais de 15 mil concessionárias na América do Norte e demonstrou que um único provedor pode comprometer a continuidade de muitos negócios.

O propósito deste texto é oferecer ao Distribuidor alguns insights que permitam uma gestão de risco cibernético de cadeia produtiva mais eficiente.

TPRM: DE OBRIGAÇÃO CONTRATUAL A ESTRATÉGIA DE SOBREVIVÊNCIA

A Gestão de Riscos de Terceiros (Third Party Risk Management/TPRM) deixou de ser um requisito de compliance para tornar-se um componente crítico de continuidade de negócios.

O National Institute of Standards and Technology (NIST) define a gestão de risco de terceiros – especialmente no contexto da supply chain - como um processo integrado ao gerenciamento de risco corporativo, que envolve estratégia, políticas, avaliação e monitoramento contínuo. De forma complementar, o National Cyber Security Centre (NCSC) do Reino Unidos estrutura o tema em quatro pilares: compreensão dos riscos, estabelecimento de controles, verificação dos arranjos e promoção da melhoria contínua.

Adaptando essas diretrizes à realidade do varejo automotivo no Brasil, a GRCIBER Soluções implementa Programas de Gestão de Riscos de Terceiros conforme a metodologia abaixo:

1. Mapeamento completo das partes relacionadas

- Identificação de todas as partes relacionadas – incluindo subcontratados – com acesso digital a sistemas, dados ou processos críticos.

2. Classificação dos terceiros segundo a sua criticidade operacional

- Avaliação do impacto operacional decorrente do comprometimento do terceiro, considerando - entre outros aspectos - a existência de alternativas operacionais e o nível de acesso a informações sensíveis. A criticidade orientará o grau de exigência contratual e técnica aplicável, em especial aos níveis de SLA.

3. Avaliação de risco proporcional

- Iniciando pelos mais críticos, avaliar o risco que cada terceiro agrega ao ecossistema utilizando ferramentas que permitam a avaliação do risco com métricas quantitativas.
- Mapeamento e a priorização dos principais eventos de risco, com especial atenção às ameaças associadas ao Ransomware.
- Não se limitar aos questionários e autoavaliações.

4. Estratégia mitigatória colaborativa

- Construir e implementar – juntamente com o parceiro – um plano para mitigação dos eventos de riscos prioritários. O modelo "impositivo" raramente funciona. A experiência internacional mostra que a construção de uma relação de confiança — com clareza de benefícios e responsabilidades — gera melhor resultado do que simples exigências contratuais.

5. Monitoramento contínuo da postura de segurança do terceiro

- O risco cibernético é dinâmico, ele muda em decorrência do surgimento de novas vulnerabilidades e evolução das ameaças. Nesse contexto, a gestão de risco de terceiros exige monitoramento contínuo (i.e., 24x7), uma vez que as avaliações pontuais são insuficientes diante de um cenário em constante transformação.

O PAPEL DA LIDERANÇA

Gestão de Riscos de Terceiros (TPRM) é um tema de governança, assim cabe à liderança – em todos os níveis – atuar para incorporar o risco cibernético de terceiros ao mapa estratégico de riscos corporativos. Isso implica:

- Conhecer os fornecedores críticos.
- Definir – de forma clara e objetiva – o apetite ao risco.
- Estabelecer critérios mínimos de segurança para fornecedores críticos.
- Inserir o processo de cyber due-diligence para novos parceiros.
- Implementar o monitoramento contínuo.

CONCLUSÃO

A pergunta deixou de ser "estamos protegidos?" para tornar-se "estamos protegidos considerando nossos terceiros?"

No cenário atual, onde ataques às cadeias de suprimentos são cada vez mais comuns, a postura de segurança dos terceiros é um imperativo para a resiliência operacional sistêmica.

Portanto, a gestão do risco cibernético das partes relacionadas é o corolário estratégico para a sustentabilidade do negócio.

Wilson Lauria é CEO da GRCIBER Soluções. Especialista em Cyber Security and Executive Strategy pela Stanford University (EUA). Professor Convidado na Escola Superior de Defesa e na Fundação Getúlio Vargas. Membro da Comissão de Gestão de Riscos Corporativos do IBGC.