Elaborado pela Comissão Regional Leste de Governança e Riscos da Abrapp

Verdade seja dita: “qualquer caminho serve para quem não sabe onde ir” (**1**). E a desorientação estratégica percebida neste ditado pode se agravar ainda mais, quando não sabemos nem onde estamos. Afinal, origem e destino são condições básicas para o estabelecimento de uma trajetória.

Então, pense nisso caso ainda não tenha razoável noção do grau de exposição de sua entidade a ataques de hackers. Provavelmente, isto esteja associado a uma tímida percepção da abrangência e da eficácia das atuais práticas voltadas para a segurança de dados em sua entidade. Portanto, um diagnóstico do ambiente de tecnologia da informação – para se conhecer a origem da trajetória – pode ser o primeiro e decisivo passo para definirmos onde vamos chegar, ou seja, a mitigação desse risco.

Abordaremos, nesta publicação, aspectos relacionados com forma, modelagem, pontos de atenção e benefícios proporcionados por um diagnóstico do ambiente de tecnologia de sua entidade.

Forma – O diagnóstico do ambiente de tecnologia pode ser conduzido tanto internamente, com equipe própria de colaboradores treinada em verificação de cumprimento e aderência de normas, quanto externamente, com a contratação de serviço de empresa especializada. Obviamente, a primeira forma de condução é uma alternativa restrita a entidades de maior porte, que possuam áreas de auditoria interna e/ou de compliance capacitadas. Sendo assim, a contratação de serviços surge como a solução mais apropriada – ou única – para a grande maioria de nossas entidades.

Em ambos os casos, os executores do diagnóstico devem se basear em modelos contendo diretrizes e requisitos auditáveis abrangendo, dentre outros temas, documentação, execução e controle de processos, ambientes de aprovação, critérios de segurança, comunicação e tratamento de incidentes, capacitação de pessoas, comumente denominados “frameworks”.

Modelagem – Existem opções consagradas de “frameworks” à disposição para esta finalidade de diagnóstico, que podem ser utilizadas isolada ou combinadamente. Nesta publicação, destacamos:

– “CIS Control” – conjunto prescritivo e priorizado de práticas recomendadas de segurança cibernética e ações defensivas, desenvolvido pela Center for Internet Security®, que pode ajudar a evitar os ataques mais disseminados e perigosos (disponível em https://learn.cisecurity.org/cis-controls-download);

– Família ISO 27000 – conjunto de normas emitidas pela International Organization for Standardization, organização não governamental com objetivo de desenvolver e promover normas que possam ser utilizadas por todos os países do mundo, neste caso com foco em tecnologia da informação, compreendendo a ISO/IEC 27001 – Tecnologia da Informação – Técnicas de Segurança – Sistemas de Gestão de Segurança da Informação – Requisitos, ISO/IEC 27002 – Tecnologia da Informação – Técnicas de Segurança – Código de Prática para Controles de Segurança da Informação e ISO/IEC 27701 – Técnicas de Segurança para Gestão da Privacidade da Informação – Requisitos e Diretrizes (disponível em https://www.iso.org/isoiec27001-information-security.html).

– NIST Cyber Security Framework – fornece estrutura e série de processos, padrões, diretrizes e práticas de segurança para organizações do setor privado nos Estados Unidos, contemplando cinco funções básicas: Identificar, proteger; detectar, responder e recuperar (disponível em https://www.nist.gov/cyberframework).

A técnica usualmente utilizada para realização deste tipo de diagnóstico consiste na realização de entrevistas com pessoas chave e obtenção, de acordo com as circunstâncias, de evidências documentais das afirmações obtidas. As entrevistas são orientadas pelos requisitos do “framework” escolhido, buscando classificá-los quanto ao grau de atendimento: Atende Plenamente, Atende Parcialmente, Não Atende ou Não Aplicável e gerar recomendações de adoção ou melhoria de

práticas não aderentes.

Veja, a seguir, exemplo de aplicação de diagnóstico:

É recomendável, ainda, a classificação dos requisitos que não atendem plenamente por prioridade de atendimento, que pode levar em consideração ações imediatas, ações de médio prazo e ações de longo prazo, conforme os níveis de criticidade e urgência dos requisitos e as precedências das ações. No nosso exemplo, caberia uma recomendação de aplicação imediata de disponibilização e divulgação da Política de Segurança da Informação, incluindo campanhas de conscientização.

Uma vez concluído, o resultado do diagnóstico é discutido com as áreas envolvidas para confirmação de sua integridade e, na sequência, apresentado à alta administração.

Pontos de atenção – O resultado de diagnóstico dessa natureza, invariavelmente, choca – e decepciona – os tomadores de decisão e colaboradores de um modo geral, em razão da elevada quantidade de “não conformidades” revelada. Desconsiderando-se os pontos fora da curva, a constatação de requisitos atendidos plenamente em organizações que realizam seu primeiro diagnóstico é significativamente inferior à de requisitos que não atendem ou atendem parcialmente. E isto é a visão do apocalipse? De forma alguma.

Primeiramente, temos que ter em mente que os “frameworks” disponíveis resultaram de pesquisas muito bem elaboradas, envolvendo instituições e profissionais renomados e com grande expertise no assunto, de modo que as práticas neles elencadas são a quintessência das melhores práticas e técnicas aplicáveis. Algo que costumamos apelidar de “Padrão FIFA”, presente em sua plenitude, talvez, somente em organizações como o “Pentágono” ou renomadas “data-ware houses”. Alguns níveis de certificação – como é o caso do TIER-IV – são inatingíveis até para grande parte das empresas de tecnologia.

Em seguida, entenda que o cumprimento irrestrito dos requisitos em sua plenitude pode levar sua entidade a um consumo de recursos muito além das suas disponibilidades orçamentárias.

Então, muita calma nessa hora. Não saia desesperado na busca de atendimento pleno de todos os requisitos. Lembre-se do seu foco estratégico que é a gestão de planos de benefícios e dos recursos garantidores desses planos. Portanto, a não ser que sua intenção seja a busca – planejada – por selo de certificação em algum “framework” de tecnologia específico ou queira mudar o foco estratégico de sua entidade – o que não é aconselhável – procure distinguir, no resultado do diagnóstico, aquilo que é necessário, aquilo que é desejável e aquilo que é dispensável em termos de segurança para entidades com a sua característica, porte, complexidade e níveis de risco. E como o diagnóstico torna-se um “revelador de dificuldades”, lembre-se de que sempre haverá alguém querendo “vender facilidades”.

Uma vez realizada a mencionada distinção, e feito alinhamento de expectativas, crie um projeto para implantação dos necessários aprimoramentos, considerando a classificação das prioridades de ações, de curto, médio e longo prazos.

E lembrem-se, a Conecta pode auxilia-los na busca por parceiros para realização deste diagnóstico.

Benefícios – A realização de um diagnóstico do ambiente tecnológico é de extrema importância para a identificação do nível de conformidade da infraestrutura tecnológica da entidade e, também, para o conhecimento – cultura organizacional – de todo o seu quadro corporativo, quanto ao tipo de ameaça que estamos expostos e possíveis soluções. Isto permitirá a redução do seu risco operacional, com reflexos diretos na mitigação do risco do negócio, conforme segue:

- racionalização da utilização do uso de recursos de tecnologia;
- melhoria no gerenciamento de capacidade de serviços de TI;
- viabilização de transição de ambiente de TI de reativo para proativo;
- transição da atuação de TI de operacional para tática e estratégica;

- melhor gerenciamento do conhecimento e de pessoas;
- melhoria na qualidade dos serviços e comunicação de TI;
- melhoria da integração entre TI e necessidades pelo porte da entidade;
- implantação de indicadores: – onde estou, para onde vou?;
- melhoria da percepção de entrega da TI; e
- solução para interrupções na disponibilidade dos serviços de TI.

Como consequência de todos os benefícios citados, podemos destacar a implementação de um processo contínuo de aprimoramento, que não se limita a apontar os impactos imediatos do ambiente de Segurança da Informação mas, a longo prazo, a trazer maior assertividade para a gestão.

Agora que você já tem condições de conhecer o ponto de origem e de vislumbrar o ponto de destino, comece a trilhar a sua trajetória rumo à mitigação do risco de ataques cibernéticos em sua entidade. Então, não perca nossa próxima publicação: – saiba como a documentação de processos pode contribuir para criar um ambiente tecnológico resiliente a ataques cibernéticos.

Nota

(**1**) Expressão eternizada em Alice no País das Maravilhas, de Lewis Carroll, derivada da célebre expressão do filósofo, escritor e político Séneca: “Não existe vento favorável a quem não sabe onde deseja ir”.

Fonte: Abrapp em Foco, em 23.06.2021