Como parte dos trabalhos das Regionais de Governança e Riscos, a Comissão Técnica Leste, sob coordenação do Antonio Carlos Bastos D´Almeida (Forluz) e Juleika Carvalho (Aceprev), elaborou o primeiro “folder” sobre o tema riscos cibernéticos, cujo texto foi também aprovado pelo Colégio de Governança e Riscos no último dia 19 de maio. Confira abaixo na íntegra:

17 de dezembro de 2016 – Fundação Libertas sofre ação maliciosa de hackers que compactaram e criptografaram arquivos dos atendentes e de mais seis máquinas de usuários, afetando o funcionamento dos seus sistemas operacionais. Resumindo, os servidores da Entidade ficaram inoperantes por quatro dias, as estações de trabalho por 15 dias e a intranet não foi mais restabelecida na sua forma original. Mensagens indicando a compactação ocorrida e e-mail de contato dos “sequestradores” surgiram nas telas dos desktops.

3 de novembro de 2020 – Superior Tribunal de Justiça brasileiro é alvo de ataque cibernético do tipo ransomware em que todo o acervo de processos da Corte foi “sequestrado”, com o uso de criptografia, sendo exigido pagamento de resgate pelos dados. Como resultado da ação, site fora do ar por 8 dias e prazos processuais, audiências e sessões de julgamento suspensos por 7 dias.

25 de novembro de 2020 – Embraer passa a operar em regime de contingência em função de ataque de hackers que invadiram sistemas e obtiveram acesso a um ambiente de arquivos da gigante brasileira de aviação, vazando informações e exigindo pagamento para resgate de dados sequestrados. A Embraer precisou desativar boa parte de seus servidores.

Em tempos de pandemia, com grande parte de nossas entidades trabalhando sob regime de contingência – home office – ações maliciosas dessa natureza se constituem nas piores ameaças à gestão dos planos de benefícios. Adicionalmente, essas ações podem trazer sérias consequências relacionadas com o cumprimento ao disposto na Lei Geral de Proteção de Dados Pessoais.

Preocupada com o fato, a Abrapp, por meio de seu Colegiado de Coordenadores de Comissões de Governança e Riscos, solicitou à sua Comissão Regional Leste estudo sobre o tema Ataques Cibernéticos, explorando os riscos dessas ações sobre a governança e gestão dos planos de benefícios. Para tanto, a Comissão programou a divulgação de uma série de pronunciamentos sobre o tema como forma de contribuir para a mitigação de riscos decorrentes desse tipo de ameaça.

Nesta primeira edição, introdutória, abordaremos aspectos conceituais básicos e considerações preliminares com o intuito de conscientizar nossas entidades acerca da gravidade dessa ameaça e da importância de planejar e implantar medidas mitigadoras. A partir das próximas edições, abordaremos ações planejadas que podem ser tomadas para mitigação desses riscos.

Conceitualmente, ataque cibernético consiste em prática utilizada por hackers para obtenção de acesso não autorizado a redes, servidores, sistemas operacionais, softwares e sites. É o que relata Wolder Fonseca, da VANTEC Soluções Tecnológicas, para quem os objetivos dessas ações são distintos, geralmente visando expor dados sigilosos, acessar, alterar, impedir ou destruir dados, vender informações com base nos dados obtidos, fornecer, impedir acessos aos sistemas (site e base de dados) ou mesmo falsificar sites para obtenção de dados bancários, dentre outros.

Andrea Melo, da A Melo IT Governance & Security Consulting, alerta para o fato de que, atualmente, estamos assistindo a uma elevação do número de ataques cibernéticos, notadamente em função do aumento de usuários trabalhando em regime de home office, por conta da pandemia.

Rodrigo Nunes, da Tripla Tecnologia da Informação e Serviços, ressalta que a frequência com que esses ataques ocorrem é muito preocupante, pois de acordo com a RSA Security, em 2020 houve um aumento de 72% nos ataques cibernéticos em todo mundo. Já no Brasil, segundo Nunes, esse aumento foi de 350%, colocando nosso País entre os mais afetados no mundo por ataques maliciosos. “É extremamente preocupante, pois estudos especializados apontam que apenas 5%

das empresas estão devidamente protegidas e preparadas para responder a um ciberataque. Um dos fatos mais importantes é que a maior parte das empresas já sofreu algum tipo de violação de segurança porém não tem CONHECIMENTO dos fatos; uma empresa que não está preparada e organizada para identificar ataques, vazamentos e ameaças é explorada por anos sem tomar nenhuma ação. ”

Os tipos mais comuns dessa ameaça, segundo Wolder Fonseca, dizem respeito a: (i) golpes de doação, tais como DDOS (ataque com intuito de “ derrubar “ou impedir” acesso aos sistemas / site) Phishing / Spear-Phishing (muito utilizado e umas das formas mais fáceis de chegar aos usuários), aplicativos móveis, Vishing (utilização de redes sociais); e (ii) Ransomware, tipo malware capaz de restringir acesso aos dados (bloqueio / criptografia) com posterior cobrança de pagamento de resgate em criptomoeda para restabelecer acesso (irreversíveis em 98% do casos). Este último merece destaque como uma das piores ameaças cibernéticas, pela sua capacidade de causar indisponibilidade de sistemas por horas, dias ou até semanas, dependendo do ambiente de contingência.

De acordo com Rodrigo Nunes, 95% das violações de segurança são causadas por erro humano e, com relação a técnicas de ataque, frequentemente são iniciadas por pessoas dentro das próprias organizações, como por exemplo, colaboradores.

Evitar ou minimizar os impactos de ações maliciosas como estas exige estabelecimento de protocolos que, segundo Andrea Melo, passam por criptografias com chaves fortes, antivírus, monitoramento de vulnerabilidades técnicas na rede interna e sistemas, conscientização de usuários, segurança em redes, equipe competente em cybersecurity, ferramentas para apoio em prevenção de incidentes para verificação de eventos de segurança da informação, dentre outras. Wolder Fonseca sugere, também, treinamento das equipes de tecnologia, manutenção atualizada dos sistemas, planos de continuidade de negócios e abolição de softwares piratas e forte política de segurança da informação. Rodrigo Nunes menciona, ainda, que “... a única forma de minimizar o risco é elevando a maturidade de segurança da informação e isso requer engajamento do CEO ao chão de fábrica. Os padrões e frameworks citados em conjunto com soluções de cibersegurança e iniciativas de conscientização têm se mostrado o melhor caminho para essa elevação de maturidade”.

Mas vamos começar a tratar essas questões a partir da nossa próxima publicação. Portanto, não percam o ... *Saiba como tirar proveito de um diagnóstico do ambiente tecnológico para planejar ações de mitigação de ataques cibernéticos*.

Lições aprendidas – Tatiane Baia Rodrigues, Gerente de Tecnologia da Informação da Fundação Libertas, salienta que importantes lições podem e devem ser aprendidas a partir de episódios como o ocorrido na sua Entidade. No que diz respeito a gestão de pessoas e conflitos, a Fundação passou a promover constante capacitação técnica e de conhecimento, integração, comprometimento, controle emocional, habilidades e relacionamento interpessoal. Com relação ao ambiente de informática, atenção maior se voltou para os aspectos de segurança e revisão periódica de políticas e boas práticas que, por sua vez, são fatores indispensáveis. Por fim, destaca a conveniência de estabelecimento de boa parceria entre fornecedores de softwares e prestadores de serviços da TI, sobretudo para solução de problemas em momento de urgência.

Fonte: Abrapp em Foco, em 25.05.2021