Por Bruna Chieco

Na atual era tecnológica, empresas e entidades devem lidar com ameaças cibernéticas sofisticadas, que crescem de maneira acelerada. Assim, as organizações não devem apenas investir em tecnologia e governança, mas sim em criar uma conscientização entre colaboradores sobre boas práticas de proteção e cumprimento de políticas internas.

O webinar “Risco Cibernético”, realizado nesta quinta-feira, 28 de setembro, teve como objetivo capacitar as Entidades Fechadas de Previdência Complementar (EFPC) na proteção eficaz contra ameaças cibernéticas e promover uma cultura de segurança digital.

Luiz Carlos Cotta, Diretor responsável pela Comissão Técnica de Governança e Riscos da Abrapp, destacou que esse é um assunto super relevante, envolvendo todos os colaboradores das fundações.

“Riscos estão presentes em tudo o que fazemos, e por isso precisamos conhecê-los todos, ou pelo menos os principais, e os que mais afetam o nosso dia a dia e as nossas atividades”, destacou, citando os riscos cibernéticos entre eles.

Cotta disse ainda que a velocidade e quantidade de acontecimentos indesejáveis nessa área são tão grandes, que de tempos em tempos a discussão sobre esse assunto se faz necessária para que seja possível se atualizar sobre o tema.

“Conversar com especialistas para trazer mais segurança às nossas entidades é essencial. Todos os profissionais devem saber sobre riscos cibernéticos, não apenas o pessoal de Tecnologia da Informação”, reiterou.

Como as ameaças são inúmeras, o webinar destacou como as entidades podem atuar, com implementação mecanismos e ferramentas de gerenciamento e estratégicas contínuas e eficazes para mitigação e prevenção de todos os riscos.

Risco estratégico – “Risco cibernético é um risco estratégico, relevante e que tem crescido, o que mostra a importância dessa questão”, reforçou Adriana Carvalho, Secretária Executiva da Comissão Técnica de Governança e Riscos da Abrapp.

Para auxiliar no tratamento desse risco, a CT desenvolveu uma série de papers acerca do assunto com o objetivo de auxiliar as fundações na implementação de todas as ferramentas e mecanismos para mitigação desse risco.

O moderador do webinar, Antonio Carlos Bastos D’Almeida, Coordenador da Comissão Técnica de Governança e Riscos da Regional Leste da Abrapp, esteve à frente de muitos desses trabalhos.

Conscientização – A Vivest criou, em 2020, um comitê de segurança da informação com participação da diretoria, com uma área de segurança da informação para tratar dos principais pilares da questão de cibersegurança.

Contando sobre a experiência, Alex Galho, CIO da Vivest, destacou que os riscos de uma entidade se dividem em infraestrutura, abarcando servidores, sistemas, e as vulnerabilidades através das quais invasores podem acessar os sistemas.

O outro lado, que é a parte mais sensível, é o de uso das próprias pessoas de dentro das empresas,

que podem ser manipuladas por atacantes para acessar os sistemas das empresas através de um método de invasão chamado de phishing.

“A gente sabe que a gente vai ser atacado, somente não sabemos como e quando”, alertou Galho. Para ele, fazer o básico bem feito em termos de proteção já ajuda. Mas, por outro lado, há um processo que ele chamou de “secar gelo”, pois por mais treinamentos que ocorram dentro das empresas, há novas ameaças que surgem a cada dia.

“Temos um monitoramento constante de nosso ambiente, buscando fazer o básico bem feito, e como entidade, temos uma grande responsabilidade com informações sensíveis”, disse, se referindo ainda às normas da LGPD.

“A segurança da informação precisa passar por um processo de desintoxicação”, disse Galho, reiterando que as pessoas precisam ver essa área como um facilitador de processos para que eles sejam seguros.

Para dar recomendações sobre como lidar com eventuais ataques e trabalhar essa conscientização dentro das entidades, o especialista Longinus Timochenco, VP Business Unit Cyber Security e Embaixador e Evangelista do CISO Forum Brazil e Diretor de Governança Corporativa Advisory, participou do webinar.

Timochenco reiterou que o elo mais fraco da segurança são as pessoas: “A maior vulnerabilidade que existe hoje, de segurança, são as pessoas. A hora que começarmos a olhar para a cibersegurança por pessoas, muitas das vulnerabilidades serão resolvidas”, disse.

Educação, portanto, é a chave para tratar dessa questão, disse o especialista. “Temos que educar, mas também responsabilizar. Todos são co-responsáveis”. Segundo ele, profissionais das empresas precisam conhecer todas as políticas de segurança antes de começar a ter acesso aos sistemas.

Ele disse ainda que é um pensamento atrasado apenas contar com um time de resposta a incidentes e combate a fraude, sendo preciso também ter um time que atua na tendência a risco. “Isso é ser efetivo e se antecipar a problemas”.

Timochenco reiterou que um programa efetivo de conscientização passa pela prática. “Praticamos segurança criando disciplina”, disse. “Por isso, é preciso educar também responsabilizando”.

Investimento – A preocupação com custos é um tema recorrente quando uma empresa trata de segurança, mas os palestrantes reiteraram que o investimento a ser feito deve ser para evitar o máximo possível os ataques.

Galho disse que as entidades precisam investir em educação e continuamente lembrar que segurança é uma atitude, um modelo comportamental. “Nunca é demais investimento em segurança da informação”,.

“O teto do investimento vai da capacidade de analisar o quanto se quer tomar risco. Não investir, ou investir somente no limite traz uma exposição desnecessária”, reiterou Galho.

Conforme o risco e a exposição aumentam, a segurança também deve aumentar, complementou Timochenco. “Temos que simplificar a questão da segurança”, disse.

O investimento também deve ser feito a partir de um diagnóstico para que as entidades saibam em que patamar de segurança e dos riscos de ameaças que elas estão, disseram os palestrantes.

“Segurança é algo vivo, que deve ser monitorado e tratado”, declarou Timochenco. “O investimento vem num processo contínuo, conscientizando as pessoas a utilizarem da melhor forma seus recursos, com cuidado, cautela e responsabilização”.

Ele ainda aconselhou: “Se vocês querem aumentar a assertividade na questão da segurança, potencialize as áreas de compliance e auditoria interna. Eles são os fiscalizadores neutros, sem conflito de interesses, e que fazem parte desse ecossistema de controle”.

Eles alertam também o custo de uma entidade ser obrigada a parar suas operações por conta de um ataque cibernético, o que pode impactar muito mais financeiramente do que investir em segurança.

Por onde começar – Para organizar a casa e passar a tratar a segurança de acordo com seu grau de importância, os especialistas recomendam o apoio de consultorias que passem um diagnóstico para que a entidade saiba onde está localizada nesta área.

“Olhar como eu estou e onde a empresa precisa chegar. A partir daí, traçamos um plano”, disse Timochenco, destacando a importância de fazer esse Raio-X para responder a essas perguntas.

Outro ponto destacado na discussão é que segurança deve ser um processo contínuo e consistente, e não apenas ações isoladas de um setor. Eles lembram que a segurança da informação é estratégica e comportamental.

Já a parte de inteligência e automatização é um segundo passo quando se trata de segurança. “Se não fizermos o básico, vamos automatizar o caos”, disse Timochenco.

Galho destacou que ter um serviço de inteligência requer pessoas especializadas. “Busque uma empresa de mercado que saiba fazer isso e entenda se você realmente precisa disso”, aconselhou.

Atualização e melhorias – Os palestrantes destacam ainda que é possível se manter informado sobre novas vulnerabilidades a partir de relatórios, buscando melhorias em seus processos de monitoramento de riscos cibernéticos. “Segurança da informação é um alerta contínuo”, disse Galho.

Também é importante ter uma lista de indicadores de incidentes que afetam o negócio ou o nicho de atuação da empresa ou entidade, disse Timochenco.

Mas eles lembram da necessidade de dar um passo anterior e fazer o básico: atualizar o ambiente, fazer a gestão de credenciais e realizar backups. “É preciso aplicar a prática que faz sentido para seu negócio. No mínimo, toda empresa deve ter uma política de segurança. Não dá mais tempo de ficar errando no básico”, complementou Timochenco.

Fonte: Abrapp em Foco, em 28.09.2023.