Conferência do Ibracon aborda o tema “cyber security”, questão essencial em um mundo cada vez mais dominado pela tecnologia e pelo trânsito de dados em ambientes virtuais

“O impacto dos riscos cibernéticos no mundo corporativo” foi o título do primeiro painel da 8ª Conferência Brasileira de Contabilidade e Auditoria Independente do Ibracon – Instituto dos Auditores Independentes do Brasil, em 11 e 12 de junho, no Teatro Bradesco, em São Paulo.

Com mediação do diretor Técnico do Ibracon Nacional, Rogério Garcia, o tema foi debatido pelo professor de Sistemas de Informação Contábil na Rutgers Business School, Kevin Móffitt; pela chefe-adjunto do Departamento de Regulação do Sistema Financeiro do Banco Central do Brasil, Paula Ester Leitão; e por Leandro Augusto Marco Antonio, representante do Ibracon e sócio líder de Cyber Securyti em firma de auditoria independente.

Paula Ester Leitão iniciou o painel com uma exposição sobre a missão do Banco Central do Brasil, que consiste em “assegurar o poder de compra da moeda e um sistema financeiro sólido e eficiente”. Tendo em vista que o ambiente bancário brasileiro é marcado pelo uso intensivo da Tecnologia de Informação (TI) e por um alto grau de interconectividade, a prevenção aos riscos cibernéticos é fator preponderante na garantia de um ambiente estável para as instituições financeiras.

“A **Resolução número 4.658**, emitida em 2018, tem como seus principais pontos, justamente, a política de segurança cibernética e a definição de requisitos para a contratação de serviços de processamento e armazenamento de dados e de computação em nuvem”, disse a palestrante. “A política de segurança cibernética prevê que a instituição deve ser capaz de prevenir, detectar e reduzir a vulnerabilidade a incidentes relacionados com o ambiente cibernético, além de estabelecer princípios e diretrizes para assegurar confidencialidade, integridade e disponibilidade dos dados e sistemas”, informou. Ainda segundo a painelista, a nova Resolução enfatiza a importância de se promover uma cultura de disseminação de segurança cibernética, com programas de capacitação e avaliação periódica, prestação de informações a clientes sobre precauções e o compromisso da alta administração com esses objetivos.

“Uma entidade que opere no ciberespaço provavelmente experienciará um ou mais eventos de violação de segurança em algum momento, independentemente da eficiência dos controles de cibersegurança desta entidade”, destacou Móffit. “Organizações podem atingir uma segurança razoável, mas não existe segurança absoluta”, prosseguiu. “É imprescindível estar preparado para detectar, responder, mitigar e se recuperar de ataques em um tempo hábil, com a menor ruptura possível em suas operações”, acrescentou.

O palestrante ressaltou que é essencial os auditores entenderem de tecnologia da informação (TI). “A auditoria de cibersegurança inclui um trabalho de gerenciamento de riscos, a verificação desse gerenciamento, a formação de uma opinião e o preparo do relatório profissional”, adicionou Móffit. “A administração é responsável por seu próprio programa de gerenciamento de riscos de segurança”, destacou.

Móffit também explicou as 10 principais ameaças à segurança em aplicativos Web, e apontou a tecnologia de blockchain como a mais segura que existe: “A rede distribuída verifica a integridade de cada transação. Além disso, transações não podem ser alteradas e são completamente transparentes”, informou. “É por isso que os reguladores, auditores e profissionais de segurança amam a tecnologia blockchain”, disse, bem-humorado.

Outra aliada contra os ataques cibernéticos é a Inteligência Artificial (AI): “Os softwares tradicionais de detecção de malware identificam assinaturas específicas e passam a monitorá-las. Já as ferramentas de AI podem aprender as características do malware, e então as escaneia em busca desses atributos. Elas podem, inclusive, ser treinadas para tomar decisões de colocar ataques em

quarentena e notificar os supervisores para intervenção".

Leandro Augusto Marco Antonio falou sobre a Pesquisa CEO Outlook, que em sua última edição trouxe alguns dados surpreendentes: 45% dos CEOs brasileiros consideram que uma eventual falha em seu sistema de segurança cibernética constitui a principal ameaça aos seus negócios, mas, contraditoriamente, 75% desses executivos acreditam que suas empresas estejam aptas a conter os impactos de um ataque desse tipo. "Em escala global, 74% dos CEOs acreditam que uma o ataque cibernético seja a principal ameaça para suas organizações, e apenas 57% confiam que suas empresas estejam aptas a conter os impactos de uma ocorrência dessas", afirmou o palestrante.

Quanto à capacidade de identificar novas ameaças cibernéticas, 91% dos CEOs brasileiros e apenas 69% dos ouvidos globalmente acreditam que suas organizações estejam preparadas para o desafio.

"Ou seja, existe a percepção de que o risco existe, mas falta uma visão mais realista acerca das possíveis respostas a essa ameaça", constatou Antonio.

A gestão dos riscos cibernéticos envolve inúmeros passos, como o desenvolvimento de uma cultura corporativa que faça com que todos sejam responsáveis pela segurança, avaliar as habilidades das equipes de TI e segurança em identificar lacunas e fazer os ajustes necessários, revisar descrições de trabalho (job description) e prover incentivos voltados à melhoria de segurança.

Fonte: IBRACON**,** em 13.06.2018.