Out/22

Cibersegurança para Conselhos

O considerável incremento dos incidentes cibernéticos tem trazido aos Conselhos um dilema de difícil solução: "Como lidar com os Riscos Cibernéticos, que exigem específicas competências técnicas, sem se envolver, em demasia, nos problemas operacionais respectivos?"

Recentes estudos indicam a necessidade de uma maior compreensão do problema por parte dos Conselhos, de modo a evitar sejam envolvidos apenas quando for tarde demais.

Estudos recentes (Forrester) indicam que o Brasil foi alvo, somente no primeiro trimestre de 2022, de cerca de 1,6 Bilhão de Incidentes Cibernéticos, o que significa 1 incidente a cada 6 segundos. Estudos globais, como o apresentado pela IBM Security em Março de 2022 (com o apoio do Instituto Poseidon) mostram um quadro semelhante, com Custo Global Médio por Violação de Dados superando os 4 MUS$ por incidente.

Estudos relacionados aos ataques de "Ramsonware" (com solicitação de resgate) indicam que 85% das empresas atacadas foram alvo de um segundo ataque e que, em caso de um novo ataque, que aceitariam pagar resgates em caso de novo ataque. Tudo indica que a situação vá se deteriorar rapidamente.

Outro elemento importante trata do desenvolvimento tecnológico dos Cibercriminosos, que tem se mostrado sempre um passo à frente dos Sistemas de Segurança das Empresas e da Capacidade de Resposta das Polícias e Órgãos de Segurança, o que antecipa um quadro de riscos cibernéticos cada vez mais complexo e elevado.

Por sorte, o desenvolvimento tecnológico de ferramentas de Ciberdefesa está bastante acelerada, porém o conjunto de ferramentas ainda é insuficiente para o combate ao Crime Cibernético.

Para incrementar sua proteção as empresas necessitam realizar uma abordagem híbrida de defesa, utilizando ferramentas tecnológicas e revisão e melhoria de seus processos ("Zero Trust" e "Zero Trust Architecture") e disciplina, criando barreiras, se não perfeitas, aumentam consideravelmente a dificuldade para os ataques dos Cibercriminosos.

Este quadro tem exigido dos Conselhos maior vigilância e seu reposicionamento para a decisão de ações preventivas de proteção da organização, antes que seja tarde demais. Neste âmbito, as Organizações necessitam que os Conselhos redefinam, o mais rapidamente possível, seu papel na proteção Cibernética das Organizações.

Estudos recentes do Gartner indicam que os Conselhos da Empresas necessitarão cada vez mais de competências disponíveis de Cibersegurança para que possam desempenhar o seu papel. O Gartner estima que, até 2025, pelo menos 40% das Empresas implementarão Comitês de Riscos Cibernéticos e eventualmente também contarão, em seus quadros, com Conselheiros Independentes com conhecimentos especializados em Cibersegurança.

De qualquer forma, a curto prazo, os Conselhos precisarão ter um maior nível de conscientização e conhecimento do universo dos riscos cibernéticos e precisarão estreitar seus laços cos suas áreas tecnológicas de informática e segurança cibernéticas de modo a antecipar potenciais riscos.

Dentro de muito pouco tempo as ações dos Cibercriminosos ultrapassarão o âmbito dos danos financeiros para passar a representar ameaças reais a vida, de funcionários e Clientes.

O Risco é Real e iminente.

Alberto Lemos Araujo Filho
Diretor Geral