Palestra sobre Cibersegurança e Mecanismos de Gestão de Risco

03 Outubro 2023

Na palestra do Engenheiro Pedro Cupertino de Miranda, Diretor de Gestão de Risco da SONAE, foram abordados diversos aspetos cruciais relacionados à gestão de riscos e à segurança cibernética. foi destacado a importância de evitar e prevenir ciberataques por meio da implementação de medidas como controle de acesso e autenticação múltipla.

Além disso, o palestrante compartilhou informações sobre um ciberataque sofrido pela SONAE em março de 2023, no qual o atacante ganhou acesso através de uma VPN e comprometeu áreas críticas, incluindo a base de dados e serviços da empresa. O ataque foi do tipo Ransomware e possivelmente originado na Ucrânia ou Rússia. O Engenheiro Miranda explicou como a SONAE lidou com a situação ativando uma equipe de gestão de risco, realizando a contenção, comunicando com as autoridades e conduzindo uma análise forense.

Um aspeto importante da palestra do Engenheiro Miranda foi a discussão sobre como a equipa de gestão de risco lidou com o ciberataque. A empresa demonstrou uma abordagem organizada e estratégica, ativando uma equipe de gestão de risco que seguiu um manual de gestão de crise bem definido. Isso facilitou a alocação de tarefas e permitiu uma resposta rápida ao incidente. Além disso, a decisão de não entrar em contato ou negociar com o atacante destacou a postura da empresa em cooperar com as autoridades. A recuperação bem-sucedida dos danos em apenas duas semanas mostrou a eficácia do plano de contingência da SONAE e a importância de uma resposta rápida e eficiente em casos de ciberataques.

As lições aprendidas incluíram a necessidade de evitar voluntarismo excessivo, garantir descanso para evitar erros involuntários, cuidar da comunicação com a comunicação social, manter transparência com autoridades, parceiros e concorrentes.

A regulamentação da União Europeia, NIS2 (Network and Information Systems), visa melhorar a segurança cibernética em setores críticos que destaca a importância do cumprimento das normas regulatórias para a proteção de infraestruturas críticas incluindo a notificação de incidentes de segurança às autoridades competentes, a implementação de medidas técnicas e organizacionais adequadas e a garantia de que as empresas estejam preparadas para enfrentar ameaças cibernéticas.

Com base no conteúdo da palestra, uma ideia para implementação seria a criação de um programa de treino focado em segurança cibernética para os colaboradores das empresas. Esse programa abordaria não apenas as melhores práticas gerais de segurança cibernética (para os colaboradores), mas também incluiria técnicas mais inovadoras e específicas sobre como identificar e responder a possíveis ciberataques. Sendo abordado tópicos como: conscientização sobre tipos de ameaças e sinais de alerta, procedimentos de resposta e simular ciberataques com regularidade.

A implementação desse programa não apenas aumentaria a conscientização e competência em segurança cibernética entre os colaboradores, mas também fortaleceria a postura de segurança geral da empresa.

Carlos Rijo - 1101626