Glossário

ALGORITMO CRIPTOGRÁFICO - função matemática utilizada na cifração e na decifração de informações sigilosas, necessariamente nas informações classificadas; - (Importante para a segurança das informações dos clientes);

ANÁLISE DE INCIDENTES - consiste em examinar todas as informações disponíveis sobre o incidente, incluindo artefatos e outras evidências relacionadas ao evento. O propósito da análise é identificar o escopo do incidente, sua extensão, sua natureza e quais os prejuízos causados. Também faz parte da análise do incidente propor estratégias de contenção e recuperação; - (Importante uma ação pré-definida para possíveis incidentes para asseguração dos clientes);

ANÁLISE DINÂMICA - tipo de teste de software que verifica seu comportamento externo em busca de anomalias ou vulnerabilidades. A análise dinâmica ocorre por meio de execução do software com dados de teste para examinar as saídas e o comportamento operacional. Ela opera como complemento da análise estática, considerando o código como uma caixa-preta. A principal vantagem da análise dinâmica é evidenciar defeitos sutis ou vulnerabilidades cujas origens são muito complexas para serem descobertas na análise estática. A análise dinâmica pode desempenhar um papel na garantia da segurança, mas seu principal objetivo é encontrar e eliminar erros, o chamado debug. Após o produto passar por um teste de análise dinâmica, ele tende a ficar mais limpo, o que traz consideráveis melhorias na performance; - (Análise importante para evitar possíveis incidentes);

AUDITORIA - processo de exame cuidadoso e sistemático das atividades desenvolvidas, cujo objetivo é averiguar se elas estão de acordo com as disposições planejadas e estabelecidas previamente, se foram implementadas com eficácia e se estão adequadas (em conformidade) à consecução dos objetivos; - (Importante que contenha um passo que garanta que tudo que foi prometido seja entregue ao usuário final com sucesso);

AUTENTICAÇÃO DE DOIS FATORES (2FA) - processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas; - (Importante a sugestão e explicação da eficácia desse passo com o aumento de bancos digitais, e também com aplicativos onde contenham informações pessoais);

BACKUP OU CÓPIA DE SEGURANÇA - conjunto de procedimentos que permitem salvaguardar os dados de um sistema computacional, garantindo guarda, proteção e recuperação. Tem a fidelidade ao original assegurada. Esse termo também é utilizado para identificar a mídia em que a cópia é realizada; - (Importante para a garantia que o cliente final não será afetado caso algum incidente da empresa acarretando perca de dados da empresa);

CERTIFICAÇÃO - atesta a validade de um documento ou entidade; - (Importante para a asseguração da empresa e demais clientes);

COMUNICAÇÃO DO RISCO - troca ou compartilhamento de informação sobre risco entre o tomador de decisão e outras partes interessadas; - (Importante para todas as partes terem consciência de tudo);

CONTROLES DE SEGURANÇA - medidas adotadas para evitar ou diminuir o risco de um ataque. Exemplos de controles de segurança são: criptografia, funções dehash, validação de entrada, balanceamento de carga, trilhas de auditoria, controle de acesso, expiração de sessão e backups, entre outros; - (Importante para expor quais são os tipos de medidas de segurança são adotados pela empresa);

INTEGRIDADE - propriedade pela qual se assegura que a informação não foi modificada ou destruída de maneira não autorizada ou acidental; - (Importante tanto quanto não ter informações apagadas é não telas modificadas por terceiros).