Plano de Gerenciamento de Riscos

Vazamento de Dados

Gravidade do Risco: Gravíssima

Descrição: O Telegram tem dados pessoais de seus usuários desde o momento do cadastro até o uso do aplicativo como mensagens, arquivos de mídia(fotos, vídeos) e até mesmo links.

Impactos: Dados de usuários como CPF, número de Telefone e fotos podem ser usadas por outros usuários de maneira indevida e ficarem expostas publicamente.

Indicadores: Usuários podem detectar se houve vazamento de dados através de recursos como Firefox Monitor, observando se seus dados foram utilizados em ocasiões não gerenciadas pelo usuário.

Estratégia de (Mitigação): Desenvolvedores e os QA(Controle de Qualidade) fazem testes diariamente em busca de aberturas na segurança do software para aperfeiçoar a criptografia.

Plano de Contingência: Encerramento do aplicativo.

Gravidade do risco:Baixa

Descrição: O telegram possui servidores para que as pessoas possam se conectar e utilizar o chat para comunicação e compartilhamento de dados.

Sobrecarga de Servidor

Impacto: O sistema pode ficar lento ou parar de funcionar devido ao alto número de usuários e dados
trafegando simultaneamente.

Indicadores: Perda de conexões, server crash, alto tempo de respostas.

Estratégias de Diminuição (Mitigação): Implementar um descarte de solicitações que ultrapassem o
tempo limite de resposta.

Plano de contingência: Abertura de mais servidores com limite de usuários reduzidos

Erro de Cryptografia

Gravidade do risco: Gravíssima.

Descrição: Uma falha de criptografia do Telegram pode deixar os dados do usuário vulneráveis para acessos indevidos.

Impacto: Violação de privacidade dos usuários.

Indicadores: Problemas de reconhecimento de dados, avisos de erros ao iniciar o aplicativo.

Estratégias de Diminuição (Mitigação): Remover o tráfego malicioso antes de fazer a descriptografia, e utilizar recursos mais avançados para esse processo, planejamento da capacidade total do tráfego de rede criptografado

Plano de contingência: Desativar o sistema até que a solução para a configuração da criptografia seja implementada.

Erro de Sintaxe (HW/SW)

Gravidade do risco: médio

Descrição: Erro Semântico(HW) é um erro na lógica de seu código digo", em sua semântica, o código está sintaticamente correto, porém não faz o que se esperava dele. Por isso, este tipo de erro é geralmente mais difícil
de ser identificado e corrigido

Impacto: Software poderá não funcionar em aparelhos mais antigos.

Indicadores: Verificar se em determinado modelo de aparelho ocorre travamento durante uso do software ou até
mesmo uma temperatura mais elevada que o normal durante o uso do aplicativo.

Estratégias de Diminuição (Mitigação): Otimização em seu código-fonte para ter um melhor funcionamento em
aparelhos mais legados

Plano de contingência: Encerramento do aplicativo para aparelhos com hardware desatualizado.

Erro de processamento

Gravidade: Grave
Descrição: É qualquer imperfeição ou inconsistência no produto do software ou em seu processo, um defeito é
também uma não conformidade.

Impactos: Problemas no processamento podem causar riscos à saúde fo software de uma empresa, mas não apenas
isso há o desgaste dos usuarios e também pode criar uma crise de credibilidade perante o mercado.

Indicadores: Produtividade, eficiência, eficácia, efetividade, qualidade, entre outros substantivos, não estão
satisfazendo os usuários do software.

Estratégias de Diminuição (Mitigação): A gestão organizacional é um fator importante no desenvolvimento de
qualquer processo, e uma forma de alcançá-la é com uma lista de tarefas. Porém, não pode ser uma composição
aleatória, sem uma linha de raciocínio, pois, caso contrário, essa elaboração será uma perda de tempo por si só.

Plano de contingência: Retornar para a versão anterior onde não ocorre esse erro.

Ataque DDOS
(Ataque Hacker)

Gravidade do risco: gravíssimo

Descrição: Ataque DDOS: Esse tipo de ataque sobrecarrega os limites de capacidade específicos de uma rede,
como a infraestrutura que suporta o site de uma empresa. O ataque DDoS envia várias solicitações para o site

Impactos: Sobrecarga de servidores;

Indicadores: Um ataque do tipo DDoS é um ataque malicioso que tem como objetivo sobrecarregar um servidor
ou um computador, esgotar seus recursos como memória e processamento e fazê-lo ficar indisponível para acesso
de qualquer usuário a internet.

Estratégias de Diminuição (Mitigação): Refere ao processo de proteger o alvo de Ataques de negação de serviço
distribuído. Ataques DDoS estão evoluindo constantemente como é da natureza da tecnologia, e também, a
motivação dos atacantes também está mudando

Plano de contingência: Melhorar a infraestrutura do servidor

Roubo de Dados

Gravidade: Gravissíma

Descrição: Trata-se de um vazamento/roubo de dados do sistema, seja por pessoas internas ou externas.

Impactos: Este tipo de problema causa instabilidade na confiabilidade do usuário em relação ao sistema, podendo
ocasionar uma perda massiva de clientes do sistema, gerando fragilidade no “Nome” da corporação e por fim
suceder a perca progressiva de arrecadação monetária.

Indicadores: Uma das formas precaver esse vazamento de dados, é utilizar a autenticação de dois fatores, sendo
eles: A tentativa de entrada em um dispositivo e a autorização em outro dispositivo previamente cadastrado.

Estratégias de Diminuição (Mitigação): Realizar backups periódicos (save in the cloud), ajuda a mitigar a perda
das conversas, arquivos e mídias em geral.

Plano de contingência: Oferecer uma uma recompensa em troca dos dados vazados

Estrutura ruim para Hardware e equipamentos

Gravidade: Grave

Descrição: A não implantação de recursos capazes, para a melhor eficiência dos equipamentos, ocasiona a incapacidade do sistema atuar em seu máximo desempenho.

Impactos: Podem ocorrer lentidões e congelamento do sistema.

Indicadores: Falha de funcionamento das estruturas.

Estratégias de Diminuição (Mitigação): Compra e manutenção das estruturas que sustentam o hardware.

Plano de contingência: Compra e renovação total de toda a estrutura utilizada

Incompatibilidade de Sistemas

Gravidade: Gravíssima

Descrição: Não funcionamento do sistema no dispositivo do usuário.

Impactos: Esse tipo de erro, pode ocasionar atraso na entrega do projeto, e possivelmente, perca de todo o trabalho
realizado na construção do sistema.

Indicadores: Sistema não abre no dispositivo.
Estratégias de Diminuição (Mitigação): Testes em todos os tipos de sistema, podem evitar esse tipo de erro.

Plano de contingência: congelamento do sistema até que o problema de incompatibilidade seja resolvido

Perda de Backup de dados

Gravidade: Gravíssima

Descrição: O risco consiste em uma perca de backups de informações que a empresa mantém em seu banco de
dados.

Impactos: Paralização das atividades corporação, causando retrabalhos e desperdício de recursos e prejuízo pela
perca de dados de valor inestimado.

Indicadores: O desaparecimento dos backups na nuvem/provedor da corporação.

Estratégias de Diminuição (Mitigação): O recurso mais utilizado é o salvamento dos backups em vários locais
diferentes, desta maneira, pode-se evitar a perca de todos os dados.

Plano de contingência: Cadastramento de novos dados, desta vez, com mais locais para armazenamento dos
backups