ProZÉto

First Issued	**04/05/2021**	**Kishi Danilo**

Summary

1. “O CASE"

O **Zé Connect** é uma plataforma de inteligência de dados de delivery de bebidas que conecta consumidores, distribuidores e entregadores com o intuito de viabilizar entregas cada vez mais eficientes e personalizadas.

E diante disso, você sabe qual é o principal combustível do Zé Connect? **O dado.**

No Zé Connect, além do volume de dados aumentar consideravelmente, dados são obtidos, manipulados, processados e armazenados todos os dias.

Neste cenário, a reputação do Zé Connect também deve ser preservada todos os dias.

Diante desse cenário, convidamos você para ajudar o Zé Connect a elaborar uma estrutura que promova através de cibersegurança, desde a concepção de uma nova funcionalidade até o armazenamento do dado...

Uma cultura de segurança baseada em transparência, inspeção e adaptação!
O que isso significa?

O Zé Connect é uma empresa jovem e que vive uma cultura de startup. Isso significa que o negócio exige decisões ágeis, pois ela lida com coisas complexas, imprevisíveis e dinâmicas demais para serem controladas.

E aí, bora ajudar o Zé Connect?

2. Imagine o produto… como você arquitetaria o Zé Connect de forma segura e adaptável para novos requisitos de segurança ao longo do tempo (Ex.: LGPD)?

Iniciaria o projeto pensando em ações básicas, pensando na privacidade do usuário e de seus dados, tais como:

- Verificar se todos os serviços e dependências que o projeto utiliza estão de acordo com a LGPD;
- Solicitar permissões de recursos do dispositivo, adotando políticas de boas práticas requerendo somente as ações necessária para o funcionamento do Zé Connect;
- Inclusão do consentimento do cliente nos termos de uso e política de privacidade, onde o usuário será obrigado a aceitar para ter acesso ao aplicativo. Nesse consentimento será especificado a finalidade e a utilização dos dados coletados, e deixando claro que o usuário poderá a qualquer momento, revogar o consentimento do tratamento de quaisquer que sejam os seus dados fornecidos, além da completa exclusão deles;
- Criar um local em que o usuário possa modificar, baixar ou até mesmo solicitar a exclusão de seus dados no aplicativo ou site;
- Utilizar um sistema seguro para armazenar os dados sensíveis do usuário.

Sendo assim, limitaria as finalidades, minimizaria os dados ao que é necessário relativamente às finalidades para as quais são processados, adotadas todas as medidas adequadas para que os dados inexatos, tendo em conta as finalidades para que são processados, sejam apagados ou
retificados sem demora, armazenar de uma forma que permita a identificação dos titulares dos dados apenas durante o período necessário para as finalidades para as quais são processados e por fim, processá-los de uma forma que garanta a sua segurança, incluindo a proteção contra o seu processamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizacionais adequadas.

3. Como você faria a educação para pessoas além dos engenheiros sobre a importância da segurança desde a concepção de novas funcionalidades?

Iniciaria com a criação de uma PSI (política de segurança da informação) que é um documento para orientar e estabelecer as diretrizes organizacionais no que diz respeito à proteção de ativos de informação, devendo, portanto, ser aplicado a todas as esferas do Zé Connect.

A PSI, deverá ser solidificada com base nas recomendações propostas pela norma ABNT NBR ISO/IEC 27001:2005, bem como estar em sintonia com a LGPD.

Uma boa PSI deve conter regras e diretrizes que orientem os colaboradores, clientes e fornecedores (bem como a própria TI da organização) com relação aos padrões de comportamento ligados à segurança da informação, condições de instalações de equipamentos, restrições de acesso, mecanismos de proteção, monitoramento e controle, entre outros cuidados imprescindíveis aos processos de negócio.

O objetivo é preservar as informações quanto à integridade, confidencialidade e disponibilidade. Um bom documento que trate de política da segurança da informação deve conter, além dos objetivos, princípios e requisitos do documento, as seguintes normatizações:

1. **Responsabilidades dos colaboradores:**
    a. *Diz respeito à imposição dos limites de uso, bem como às responsabilizações em caso de má utilização dos recursos de TI da empresa. Nesse trecho, poderão ser inseridos regramentos com relação à impossibilidade de uso de dispositivos externos em equipamentos corporativos, informações sobre websites de acesso proibido, recomendações de preservação do maquinário da empresa etc.*

2. **Responsabilidades da área de TI:**
    a. *Organizar a logística da TI da organização, configurar os equipamentos, instalar softwares e implementar os controles necessários para cumprir os requerimentos de segurança estabelecidos pela política de segurança da informação são fundamentais para que o documento elaborado tenha vida e funcionalidade na dinâmica da empresa.*

3. **Informações ligadas à logística da implementação da TI na organização:**
    a. *Refrigeração de data centers, gestão de aplicações, organização física dos ativos de rede, recomendações de procedimentos etc. Tudo o que for relacionado à implementação da infraestrutura de TI na organização pode ser descrito nesse capítulo, o qual servirá como norte.*

4. **Tecnologias de defesa contra ciberataque:**
    a. *Big Data Analytics contra crackers, firewall, criptografia, controles de acesso, backups, auditorias, monitoramento de rede.*

5. **Política de treinamento aos colaboradores:**
    a. Não basta implementar uma infinidade de sistemas de monitoramento de rede, recursos para verificação de ameaças em potencial, firewalls e serviços de Cloud Security. É necessário, portanto, treinamento constante e conscientização de equipes, que podem ser previstos na política de segurança da informação.
    b. Um plano de treinamentos de longo prazo que pode ser definido através da PSI, tendo como objetivo principal auxiliar cada funcionário a extrair de sistemas o melhor para aumentar sua produtividade dentro da empresa.
    c. Além de despertar sua ciência sobre os riscos de fazer downloads por fontes desconhecidas, clicar em links não confiáveis, visualizar o conteúdo de spams, etc.

4. Quais práticas de segurança você consideraria para o processo de desenvolvimento.

A qualidade de um programa pode ser mensurada de diversas maneiras. Estabilidade, confiabilidade, baixo número de falhas e atualizações constantes são algumas das caraterísticas que definem um bom desenvolvimento.

Na era da informação, os ataques a dispositivos e aplicações são cada vez mais frequentes. Nesse cenário, o desenvolvedor é obrigado a oferecer aplicativos mais seguros para os seus usuários.

E quando falamos do cenário Brasileiro, um dos países mais vulneráveis do mundo, a implementação de processos de segurança e as boas práticas de desenvolvimento tornam-se ainda mais importantes. Abaixo irei pontuar algumas boas práticas no processo de desenvolvimento, assim como:

1. **Flexibilidade:**
    a. *Um dos principais pontos para trabalhar de maneira inteligente no gerenciamento de desenvolvimento de softwares é sendo flexível. Hoje, cada projeto exige uma metodologia única, que seja adaptada às necessidades do usuário e consiga entregar uma aplicação inteligente e inovadora.*

2. **Adote indicadores de desempenho (KPI's):**
    a. *Os indicadores de desempenho são uma estratégia inteligente e disseminada amplamente no mercado, para que empresas possam ter uma visão abrangente sobre vários aspectos do negócio.*

3. **Criar uma granularidade nos projetos:**
    a. *Durante o planejamento, busque criar um projeto com mais etapas. Essa abordagem dá mais flexibilidade ao negócio, que conseguirá avaliar melhor a qualidade do produto que está sendo criado e as chances de o sistema atender à demanda de usuários, clientes e parceiros comerciais.*

4. **Tenha ferramentas para distribuição de tarefas:**
    a. *Um dos pontos principais da gestão de projetos é a divisão de rotinas entre cada time. Essa atividade, em princípio, simples, tem um impacto direto na capacidade do negócio de se manter funcional, com alta produtividade e livre de erros.*

5. **Escolher uma metodologia que se alinhe ao objetivo:**
    a. *Um dos pontos chaves da criação de um sistema é a escolha da metodologia a ser utilizada. É importante que os métodos adotados estejam alinhados com os objetivos, além de serem capazes de entregar uma aplicação que consiga corresponder aos requisitos corretamente.*

6. Se imagine sendo o Engenheiro de Cibersegurança do Zé Connect… Quais são os principais danos para esse produto e que cibersegurança deveria evitar?

Para um bom projeto de SI e/ou Cibersegurança sempre devemos nos basear nos pilares da segurança:

- ***Confidencialidade;***
- ***Integridade;***
- ***Disponibilidade.***

Ou seja, é necessário que as ações realizadas se dediquem a garantir esses três aspectos anteriores. E não é difícil compreender seu contexto na área.

Um erro de confidencialidade pode expor dados estratégicos da organização para concorrentes, ou então um vazamento de dados de clientes realizado por hackers. Esse tipo de problema gera prejuízos financeiros e problemas com a imagem da corporação no mercado, evidenciando as falhas de segurança para o público.

A integridade das informações também é essencial. Por exemplo, um erro no disco rígido pode corromper determinados arquivos importantes. Sem um backup, as funções da empresa podem ficar comprometidas.

Disponibilidade é outro ponto essencial, já que os dados precisam estar acessíveis quando foram requisitados, principalmente para garantir a agilidade dos processos. Isso pode ser impedido, por exemplo, por ataques de sequestro de dados (ransomware), que tem justamente a indisponibilidade como objetivo.

E, em tempos de redes sociais, uma informação pode ser propagada rapidamente, gerando uma imagem ruim da área de segurança da informação da empresa, manchando seu nome como profissional. Portanto, é imprescindível que as ações a serem implementadas na área de segurança priorizem sempre estes três pilares.

7. **Imagine casos infelizes… supondo que algum dado sensível (Ex.: Nome, CPF e e-mail) de algum usuário seja armazenado em algum servidor de logs centralizado, como você identificaria esse dado e tomaria alguma ação?**

Para ser evitado esse tipo de situação, verificaria a possibilidade de implantação de um SIEM, para correlação de eventos, análise de vulnerabilidades dos ativos (bancos de dados, aplicações, endpoint etc.), análise de conformidades dos sistemas operacionais, criação de um comitê de segurança da informação (CSI), adotaria também uma gestão de riscos em seis etapas:

- **Identificação de riscos**: identificando todas as ameaças que falhas em sistemas da TI podem ocasionar na empresa.
- **Avaliação dos riscos:** qual é a gravidade de cada risco identificado na etapa acima? Aqueles que tiverem maior impacto devem ser priorizados, isto é, será necessário tomar ações imediatas.
- **Mitigação de riscos:** implementar medidas preventivas para reduzir a probabilidade de ocorrência do risco e limitar seu impacto.
- **Desenvolvimento de resposta a incidentes:** estabelecer planos para gerenciar um problema e recuperar suas operações.
- **Desenvolvimento de planos de contingência:** garantir que a empresa possa continuar funcionando após um incidente ou uma crise.
- **Monitoramento de riscos:** constantemente verificar a eficácia das estratégias adotadas para gerenciar os riscos identificados nas primeiras etapas. Além disso, é importante sempre avaliar a possibilidade de novas ameaças e se há riscos que não haviam sido identificados.

Também estudaria a viabilidade junto aos gestores, para criação de um NOC/SOC, para analise tanto de eventos de Redes como de Segurança, e monitoramento proativo de incidentes.