Empresa

A empresa que foi escolhida para criar as políticas de segurança foi a **Sinapse Digital Ltda.**, que é uma empresa destinada a desenvolver softwares, tais como um projeto de uma plataforma para freelancer, fácil de usar, e que mostre projetos em que o freelancer está participando.

Politica de Segurança

Criptografia e Hash

Dados devem, sempre que possível, ser criptografados de maneira a serem descriptografados e mostrados apenas para o usuário dono dos dados.

Política de senhas

As senhas utilizadas devem conter de 6 a 12 caracteres alfa numéricos, variando entre maiúsculas e minúsculas, evitando padrões. As senhas **não** devem ser repassadas para outras pessoas.

Devem ser permitidas apenas senhas como descritas acima, e que sejam diferentes para desenvolvimento, homologação e produção.

Senhas não devem **nunca** serem utilizadas dentro do código.

Política de e-mail

Proibir a abertura de e-mail com extensões de anexos dos tipos `.bat`, `.exe`, `.lnk` e `.com`, exceto, se esse conteúdo foi solicitado.

E-mail que não forem estritamente sobre os trabalhos, ou demais necessidades da empresa, devem ser evitados.

Politicas de acesso à internet

Os sites acessados devem ser relacionados a documentações, tutorias e downloads de dados relacionados somente a programação dos produtos.

Sites que envolvam pornografia, jogos, bate-papo, apostas, não poderão ser acessados.

Ferramentas P2P também são proibidas.

Politica de estação de trabalho

Fazer logoff sempre que sair da máquina.

Não instalar softwares que não sejam restritos ao desenvolvimento dos softwares.

Filmes e músicas, em qualquer formato, ou qualquer pirataria são proibidos.

Política social

- Não comentar sobre as políticas de seguranças para terceiros, ou em locais públicos.
- Nó divulgar ou usar as senhas em outros locais.
- Aceitar somente de membros da equipe identificados.
- Não fazer procedimentos técnicos vindos de e-mails.

Vírus

- Proibido instalar programas que não voltados para o desenvolvimento dos softwares.
- Manter os antivírus atualizados.
- Não usar e trazer cd's de fora da empresa.
- Quaisquer atitudes estranhas, chame a equipe técnica.

Autorização e autenticação de usuários

As senhas não podem ser armazenadas sem algoritimos de hash seguro. Deve-se, também, haver controle de senha e usuário para determinar o usuário que está utilizando o sistema.

Ferramentas como `0Auth2` devem, sempre que possível, ser utilizadas.

Certificados digitais (como o `ssl`) devem ser adotados.

Padrões de desenvolvimento

Para segurança, tanto dos clientes, quanto dos desenvolvedores, padrões de desenvolvimento como:

- A escrita em armazenamento não pode ser acessado por outras maneiras diferentes do que senhas.
- Informações (devem preferencialmente) ser salvas de criptografadas.
- Proibir maneiras de **SQL Injection** (que são comandos Data Definition Language injetados e rodados no sistema), que pode inserir ou alterar dados, portanto maneiras como parametrizar consultas, evitar entradas desnecessárias do usuário, limitando privilégios de acesso e usando **"stored procedures"**.
- O acesso banco não pode ser acessado utilizando um usuário com permissões de root. Devem ser permitidos acessos extremamente necessários para o uso do sistema.
- Assim como ataques de **SQL Injection** são evitados, injeção de HTML e Javascript, e do tipo cross-site scripting (XSS) também deve ser prevenidos.

- Outras categorias de ataques a serem testados são os de quebra de autinticação e de gerenciamento de sessão.

Código-fonte

O código-fonte do sistema deve estar em um versionamento, preferencialmente em um sistema de versionamento distribuído, para recuperação de possíveis falhas.

Ambientes

Para cada ambiente (desenvolvimento, testes e homologação) devem ser utilizados banco de dados e servidores de aplicação/testes distintos para cada ambiente.

Comunicação servidor-cliente

A comunicação entre servidor e cliente deve ocorrer de maneira segura, portanto, certificados digitais, controle de perda e duplicação de informações devem ser utilizados.

O armazenamento dos dados em ambos os lados (cliente-servidor) deve ocorrer de maneira segura, e transmitidos de igual forma.

Podem ser utilizados logs confiáveis para confirmação de entrega e recepção de dados.

Os logs também podem ser aplicados em situações como:

- Login e logout do sistema
- Acesso a determinadas telas do sistema
- Acesso a informações sigilosas
- Inclusão, alterações, ou exclusão de dados do banco de dados.

Backups

- Criar e fazer a manutenção de backups, tanto de dados, quanto de códigos-fonte, tendo inclusive, políticas de acesso aos mesmos. Devem haver versionamento dos mesmos, e responsáveis capacitados responsáveis pela recuperação.

Testes

- Testes devem sempre ocorrer, antes de cada versão que modifique a estrutura (como telas de login, serviços não autenticados).
- Além dos anteriormente citados, testes automatizados para averiguar se os dados sigilosos estão indo corretamente só para o detentor da informação.
- Outra metodologia que deve ser utilizada é a de ter uma equipe focada em segurança, que faça testes, assim evitando possíveis erros deixados pelos programadores.
- Cenários de testes, como versões de banco de dados, servidores de aplicações, versões de browser, ou de sistemas operacionais, devem ser averiguadas para testar possíveis erros, e vulnerabilidades.

Ocorrências

Caso ocorram falhas mesmo aplicando as políticas anteriormente citadas, devem haver manutenção corretiva e acompanhamento pós-invasão.

Essas ocorrências devem ser anotadas, de maneira a revisar a política, ocorrendo posteriormente, testes e novas práticas incrementais para a segurança do sistema.

Criador

Olá me chamo Gustavo, e criei este material, para mais informações, clique nos links abaixo:

- LinkTree
- Disponível em : Repositório de exercícios