**PIA Goal**

**2) Initial risk assessment for a plan setup withou any corrective measures(e.g. data storeed in clear texto, insecure communications) using tool [3]**

**This should include the definition of Likelihood and Severity of the identified risks, leadint to a privacy risk matrix (risk mapping[3])**

O sistema atualmente configurado não tem medidas de segurança e corretivas adicionais. O que quer dizer que os dados pessoais identificáveis (PII) estão sendo armazenados em texto claro. As comunicações entre dispositivos e servidores são feitas através de conexões inseguras (não criptografadas).

Vamos avaliar o nível de risco, em termos de ‘likehood’ e ‘severity’ os riscos dados e aqueles que achamos por bem adicionar.

1. Um risco que está inerente, é a **perda de controle sobre os dispositivos emprestados** pois estes podem ser perdidos ou roubados durante a semana da campanha. Desta forma este risco tem uma likelihood média. Como a perda deste poderia expor informações sensíveis, tem uma severity alta.
2. Outro risco que tem likelihood médio será a **fraca gestão das permissões**. A gestão das permissões é feita através de uma aplicação nova, a COP-NVM. Os participantes não sendo instruídos a usa-las poderão não estar a usar a aplicação no seu potencial, fazendo com que a informação coletada não seja tão útil quanto poderia ser. A severity é baixa.
3. A **segurança da conectividade e transmissão de dados**, é um risco, que por falta de medidas de segurança, encontra-se com uma likelihood alta, pois conexões não seguras são comuns e fáceis de explorar. A sua severity é também alta, porque a interceptacão de dados pode levar à exposição de informações sensíveis.
4. **Armazenamento e segurança dos dados.** Este risco depende muito das mas medidas de segurança implementadas, mas não existindo nenhuma tem uma likelihood média, pois os dados poderão ser acedidos facilmente. Quanto à severity é alta, pois caso os dados não estejam seguros, a privacidade dos participantes estará comprometida.
5. **Acesso por terceiros e compartilhamento de dados.** No fornecimento de dados a terceiros os acordos deverão estar bem definido no que diz respeito ´

à utilização dos dados dos participantes e a forma como estes são partilhados. Tem uma likelihood baixa, pois esses acordos parecem estar em vigor, mas a severity é alta, pois dados compartilhados de maneira inadequada podem levar a violações de privacidade.

Para além destes riscos, temos aqueles identificados pela pia que são o acesso ilegítimo de dados, modificação indesejada dos dados e desaparecimento dos dados:

1. **Acesso ilegítimo dos Dados**

Tendo a informação guardada na base de dados como clear text, ter acesso a este constitui um risco enorme, pois os dados são facilmente legíveis. Desta forma, tem uma likelihood alta, visto que a privacidade dos participantes estará automaticamente frágil. Isto poderá ter consequências graves como a de sequestro. O acesso a dados de localização, por exemplo, representa um perigo para os participantes. Este risco tem assim uma severity alta.

1. **Modificação Indesejada dos Dados**

A possibilidade de modificação dos dados, sem controlo de acesso e auditoria regular tem um likelihood médio. Se isto ocorrer, pode invalidar a integridade dos dados de pesquisa. Isto leva a conclusões erradas e potencialmente afeta a credibilidade do projeto. Tem uma severity média.

1. **Desaparecimento dos Dados.**

O desaparecimento dos dados pode ser acidental por parte de um trabalhador, considerando o ciclo de vida dos dados no projeto. Porém a facilidade e a falta de segurança no acesso a estes, pode também ser um fator importante. Sem medidas de segurança este risco tem likelihood médio. Se os dados forem críticos para a pesquisa, ou irrecuperáveis, a credibilidade do projeto poderá ser vulnerabilizada, e questões legais poderão ser levantadas. O impacto operacional poderá ser grande, assim como custos de recuperação. Além disso, as consequências legais poderão por em causa a sobrevivência do projeto. Desta forma, a severity deste risco é alto.

A seguir, temos a tabela de riscos:

| **Risco** | **Likelihood (1-3)** | **Severity (1-3)** |
| --- | --- | --- |
| Perda de Controle sobre Dispositivos | 2 | 3 |
| Fraca gestão das permissões | 2 | 1 |
| Armazenamento e Segurança dos Dados | 2 | 2 |
| Segurança da Conectividade | 3 | 3 |
| Acesso por Terceiros e Compartilhamento de Dados | 2 | 3 |
| Acesso Ilegítimo aos Dados | 3 | 3 |
| Desaparecimento de Dados | 2 | 3 |
| Modificação Indesejada de Dados | 2 | 2 |

3) **A plan of action ( corrective measures) to adress the identified risks.**

Vamos agora, para cada risco identificado em cima, apresentar possíveis medidas de forma a mitiga-los e tornar o projeto mais seguro.

|  |  |
| --- | --- |
| Riscos | Medidas de mitigação |
| Perda de Controle sobre Dispositivos | * Controle físico e segurança do dispositivo: Implementar funcionalidades de bloqueio remoto e ativar medidas anti-roubo que permitam apagar dados remotamente em caso de perda ou roubo. * Autenticacão forte: Configurar autenticação multifatorial para acessar o dispositivo. Por exemplo, um pin e impressão digital. |
| Fraca gestão das permissões | * Dar instruções claras de como o aplicativo COP-NVM funciona de forma a coletar os dados de forma eficiente. |
| Armazenamento e segurança dos dados | * Utilizar soluções de ‘Database Activity Monitoring’ para monitorar e auditar o acesso a e as alterações nos banco de dados. * Gestão de chaves de criptografia: Implementar uma gestão de chaves robusta que assegure a criação, armazenamento, distribuição e destruição segura das chaves de criptografia. * Utilizar algoritmos de criptografia fortes, como AES-256, pata criptografar todos os dados armazenados nos dispositivos e servidores. |
| Seguranca da conectividade e transmissão de dados | * Implementar VPNs (Redes Privadas Virtuais) para criar um canal seguro de comunicação para transmissão de dados sensíveis. * Usar TLS (Trasnport Layer Security) ou SSL (Secure Sockets Layer) para criptografar todos os dados transmitidos entre os dispostivos e os servidores. * Aplicar listas de controlo de acesso(ACLs) e firewalls para restringir quem pode acessar a rede e os serviços. * Encriptar com criptografia simétrica. (mais detalhado a frente). |
| Acesso por terceiros e compartilhamento de dados | * Garantir que todos os terceiros que têm acesso aos dados assinem acordos de confidencialidade e não divulgação * Incluir cláusulas específicas que delineiem o uso apropriado dos dados e as consequências de violações * Usar métodos de transferência de dados seguros, como HTTPS, para garantir a criptografia dos dados durante a transferência. * Estabalecer canais seguros de comunicação, através de redes privadas ou VPNs. * Antes de compartilhar os dados, remover ou modificar informações identificáveis para proteger a identidade e privacidade dos participantes. |
| Acesso ilegítimos dos dados | * Implementar **autenticação multifatorial** para todos os usuários ao acessarem sistemas que contêm dados sensíveis. * Criptografar os dados sensíveis em repouso, usando encriptação assimétrica, e gerir a distribuição de chaves de forma a garantir que quem tem acesso às chaves são as pessoas que tem a autorização para usar os dados sensíveis. * Instalar e configurar firewalls e sistemas de prevenção de instrusões (IPS) para monitorar e bloquear atividades maliciosas * Aplicar técnicas de anonimização de forma a não comprometer a integridade ou a utilidade dos dados. Isto pode ser feito através de uma pseudonimizacão, onde se substitui identificadores diretos por pseudônimos, que não podem ligados de volta a um indivíduo sem uma chave adicional. Ou ainda com alteração dos dados sensíveis de forma que a informação original seja obscurecida. |
| Modificacão Indesejada dos Dados | * Implementar hashes criptográficos para verificar a integridade dos dados durante o armazenamento. Isto pode ser feito usando algoritmos de hashing como o SHA-256 para criar um checksum dos dados que possa ser verificado regularmente. A função de hash pode ser útil devido à sua resistência a colisões e à sua capacidade de produzir um hash único para cada conjunto de dados. Caso os dados sejam alterados então a hash será diferente, detetando então essa mesma modificação. * Para facilmente obtermos os dados antes da modificação, um processo eficaz seria a realização de backups regulares * Para monitorizar todas as atividades, uma configuração do sistema de monitoramento e logging, de forma a registrar todas as atividades de acesso e modificação dos dados. |
| Desaparecimento dos Dados | * Implementação de sistemas que detetam e alertam sobre atividades anormais que podem indicar riscos de perda de dados. * Utilizar tecnologias como RAID (Redudant Array of Independent Disks) para armazenar dados em múltiplos discos, o que proporciona protecão contra falhas de hardware. |

Além destas medidas relativas aos riscos identificados, vamos também analisar os seguintes riscos, dados no tarefa :

Data leak thorough eavesdropping of communications between smartphones and the project server.

Medidas de mitigação: Podemos implementar TLS (Transport Layer Security) para todos os dados em trânsito entre os smartphones e o servidor do projeto, garantindo que o canal de comunicação seja criptografado. Isso é alcançado usando cifras fortes, como AES com chaves de 256 bits, para uma criptografia robusta e segura. O TLS utiliza criptografia assimétrica durante o handshake para estabelecer uma conexão segura, onde as chaves públicas e privadas são usadas para trocar uma chave simétrica segura.

Quanto à geração de chaves simétricas, estas devem ser criadas usando um software de gerenciamento de chaves confiável, onde cada chave é única e utilizada apenas para uma sessão ou um conjunto limitado de dados para manter a integridade e a segurança. Podemos empregar um protocolo de acordo de chaves, como Diffie-Hellman, para estabelecer uma chave simétrica compartilhada entre o dispositivo do participante e o servidor do projeto de forma segura. Isso permite que as duas partes concordem com uma chave comum sem a necessidade de transmiti-la diretamente, evitando assim sua intercetação. A comunicação inicial é protegida por TLS, que também garante a autenticidade do servidor através de certificados digitais confiáveis e atualizados regularmente.

**Data leak from unauthorized server/data access. Access to the stored data should be limited to authorized users and the server should be accessible remotely, but not exposed/accessible directly to from the outsider.**

Para mitigar o risco de vazamento de dados devido ao acesso não autorizado ao servidor ou aos dados armazenados, podem ser implementadas as seguintes medidas de mitigação:

1 - Controle de Acesso Baseado em Funções (RBAC): Implementação de sistemas RBAC para garantir que apenas usuários autorizados tenham acesso ao servidor e aos dados.

2 -Autenticação Multifatorial (AMF): Utilização de AMF para todos os acessos ao servidor, reforçando a segurança com uma camada adicional de autenticação.

3 - Rede Privada Virtual (VPN): Estabelecimento de um ponto de acesso VPN seguro para acesso remoto, o qual os smartphones dos usuários deverão conectar, assegurando a proteção dos dados em trânsito.

4 - Segurança de Protocolo IP (IPsec): Configuração do IPsec para adicionar segurança nas comunicações de rede, protegendo os dados através de encriptação e autenticação.

5 - Associações de Segurança (Security Associations - SAs): Definição de SAs para estabelecer os parâmetros da comunicação segura, o que inclui a seleção de algoritmos de criptografia, chaves e métodos de autenticação.

6 -Internet Key Exchange versão 2 (IKEv2): Implementação do protocolo IKEv2 para a troca e renovação seguras de chaves criptográficas.

Para completar, é vital garantir que as políticas de segurança da informação e as configurações de rede sejam revisadas e atualizadas regularmente para acompanhar a evolução das ameaças e das tecnologias de segurança. A combinação destas estratégias fornece uma abordagem robusta para proteger os dados contra acessos indevidos, tanto em repouso como em trânsito.

4) **Risk assessment for an improved setup with application of corrective measures. Assessment/evaluation of the risks with the corrective measures using tool [3].**

Vamos analisar os riscos identificados anteriormente (no ponto 2) e analisar a sua ‘likelihood’ e ‘severity’.

| **Risco** | **Likelihood (1-3)** | **Severity (1-3)** |
| --- | --- | --- |
| Perda de Controle sobre Dispositivos | 2 | 1 |
| Fraca gestão das permissões | 1 | 1 |
| Armazenamento e Segurança de Dados | 1 | 1 |
| Segurança da Conectividade | 1 | 1 |
| Acesso por Terceiro e Compartilhamento de Dados | 1 | 2 |
| Acesso Ilegítimo aos Dados | 1 | 2 |
| Modificação Indesejada dos Dados | 1 | 2 |
| Desaparecimento de Dados | 1 | 2 |
| ‘Data leak thorough eavesdropping of communications between smartphones and the project server.‘ | 1 | 2 |
| ‘Data leak from unauthorized server/data access. Access to the stored data should be limited to authorized users and the server should be accessible remotely, but not exposed/accessible directly to from the outsider. ‘ | 1 | 2 |