Universidade do Minho
Escola de Engenharia

UNIVERSIDADE DO MINHO

Trabalho Pratico – Aula 6

Autores:

Bruno Rodrigues: pg41066

Carlos Alves pg41840

1 ÍNDICE

2 PERGUNTA 1.1

Primeiramente, o RGPD exige a todo o responsável, regras e procedimentos do ponto de vista tecnológico de modo a que este aplique medidas/técnicas e organizativas adequadas a assegurar e a comprovar que o tratamento dos dados é efetuado dentro da conformidade.

Com isto aparece a técnica pseudonimização que se baseia no tratamento dos dados pessoais de forma que deixem de poder ser atribuídos a um titular especifico sem recorrer a informações suplementares, a única regra é que estas informações suplementares tem de ser mantidas separadamente e sujeitas a medidas técnicas e organizativas para assegurar que os dados pessoais não sejam atribuídos a uma única pessoa identificada ou identificável.

Esta técnica tem vindo a ser utilizada pelas organizações para satisfazer os preceitos impostos pelo RGPD. De tal modo a pseudonimização deve atingir tais objetivos:

- Não pode ser possível conseguir identificar o pseudónimo, nem dentro de um contexto específico de processamento de dados também ele específico.
- Não deve ser trivial para qualquer terceiro reproduzir os pseudónimos.
- Uma abordagem de pseudonimização também pode gerar ganhos adicionais na proteção de dados em termos de precisão dos dados.

Certos aspetos necessitam de ser cuidadosamente considerados pelo controlador de dados antes de selecionar uma técnica específica de pseudonimização.

A técnica de ***Hashing*** pode ser usada na derivação dos pseudónimos, porem é necessário ter em atenção á escolha do algoritmo/função criptográfica, pois o SHA-1 e MD5 não devem ser usados, mas os o SHA-2 e o SHA-3 já podem. Além disto, esta técnica peca em ambas as propriedades, pois é trivial ser verificado por qualquer agente externo e ainda é possível aplicar a mesma função *hash* ao mesmo identificador, por consequente recebendo o mesmo pseudónimo. Estas desvantagens podem ser facilmente ultrapassadas usando *hash* com *salt*, deste modo valida as duas principais propriedades (D1 e D2), pois torna-se possível produzir vários pseudónimos diferentes com o mesmo input, o adversário não conhecendo a chave também não poderá identificar o mesmo. Usando um *salt* aleatório teremos ainda mais vantagens.

A utilização de cifras também é considerada uma técnica para alcançar a pseudonimização. Aqui teremos então **as cifras simétricas e assimétricas**, ambas podem ser empregues nestes casos. Nas simétricas o identificador do individuo é cifrado por um algoritmo de encriptação simétrica, o resultado dessa cifragem é usado com o respetivo pseudónimo. A propriedade nestas cifras é salvaguardada até que um terceiro tenha conhecimento. Nas assimétricas, são usadas as técnicas de par de chave publica/privada.

É possível que a organização desenvolva a sua própria técnica, seja ela uma combinação de esquemas criptográficos, **soluções descentralizadas** (cada utilizador gera e controlo os próprios

pseudónimos), **tokenisation** (processo onde os dados dos indivíduos são substituídos por tokens), **Masking**, **Scrambling** e **Blurring** sendo estas três últimas as mais restritas no contexto da pseudonimização.

3 PERGUNTA 1.2

3.1 CASO DE USO: GESTÃO DE SALÁRIOS

Nesta secção é avaliado o processamento de dados realizado para o pagamento de salários, segurança social e benefícios por uma PME e a sua segurança ao realiza-lo.

São considerados o processamento dos dados necessários dos trabalhadores, como contacto, NIF, NSS, e também a sua senioridade, posição e salário.

Este processamento é realizado pelos Recursos Humanos, que trata e processa a informação necessária. Neste caso, existe uma Política de Uso em prática, mas não existe políticas sobre retenção de dados ou a sua destruição. Processamento de dados pessoais só são realizados na empresa. Mesmo existindo uma clausula de confidencialidade, os Recursos Humanos não têm nenhum treino referente a segurança e proteção de dados.

O documento segue uma metodologia de avaliação de impacto que é definida da seguinte forma:

- Baixo – Podem ser encontradas pequenas inconveniências, que podem ser ultrapassadas facilmente. Um exemplo seria a reintrodução de dados.
- Medio – Podem ser encontradas inconveniências significantes, que são possíveis ultrapassar com alguma dificuldade. Neste espetro encontra-se, por exemplo, custos extras, Denials of Service.
- Alto - Podem ser encontradas inconveniências significantes, que são possíveis ultrapassar com bastante dificuldade. Um exemplo seria a entrada numa lista negra por instituições financeiras, danos, desfalques financeiros.
- Muito alto – Podem ser encontradas inconveniências significantes, ou irreversíveis, que podem não ser ultrapassadas. Neste espetro podemos encontrar, por exemplo, morte, danos físicos ou psicológicos permanentes.

Analisando o caso de uso, tendo em conta o método de avaliação de impacto descrito em cima, podemos identificar o seguinte:

- **Perda de confidencialidade**
  Analisando o processo de gestão de salários realizado no caso de uso, a perda de confidencialidade está principalmente relacionada com a divulgação de informações acidental a terceiros. Isto pode levar com que os trabalhadores que tenham as suas informações divulgadas tornem-se alvos de roubos, logo o impacto da perda de confidencialidade está avaliado como Médio.
- **Perda de integridade e disponibilidade**

A perda de integridade e disponibilidade é considerada como baixo, de acordo com a metodologia de avaliação de impacto, devido ao facto que estes problemas costumam ser pequenos inconvenientes, como atraso de pagamentos, ressubmissão de informação no sistema, que são facilmente ultrapassadas.
A avaliação geral do impacto normalmente é avaliada com a nota do risco mais alto identificado. Neste caso o impacto geral será médio.

Probabilidade de ocorrência de ameaças

A avaliação da probabilidade de ocorrência de ameaças é baseada nas questões presentes na secção 2.1.3.

Este processo de avaliação está dividido em quatro áreas principais (áreas a avaliar) sendo estas as seguintes:

- Rede e recursos técnicos
- Processos / procedimentos relacionados a operações de processamento de dados
- Diferentes partes e pessoas envolvidas na operação de processamento
- Setor comercial e escala do processamento

Cada uma destas áreas tem 5 perguntas à qual tem de ser respondidas, neste caso com um sim ou não.

Respostas positivas (em que a resposta é sim), corresponderá a uma falha.

A determinação do risco em cada área corresponde ao número de respostas positivas dadas, sendo que estas se dividem com a seguinte escala:

- Uma resposta positiva, a probabilidade será baixa
- Duas respostas positivas, a probabilidade será media
- Três respostas positivas, a probabilidade será alta

Em termos de probabilidade de ocorrências de ameaças de forma geral, a escala é a seguinte:

- 4 a 5 a probabilidade de ocorrência será baixa
- 6 a 8 a probabilidade de ocorrência será media
- 9 a 12 a probabilidade de ocorrência será alta

Passamos então a avaliação da probabilidade de ocorrência de ameaças no caso de uso em estudo.

Na área de “Rede e recursos técnicos” a probabilidade de ocorrência é baixa, visto que o sistema não está conectado à internet e não permite acesso a partir internet a recursos internos e outros sistemas de IT. Assume-se também que o acesso não autorizado é prevenido através do seguimento de boas práticas de segurança.

Na área de “Processos / procedimentos relacionados a operações de processamento de dados“ a probabilidade de ocorrência é baixa, sendo que se assume que as funções e responsabilidades

dos Recursos Humanos estão claramente definidas, que existe uma política de uso aceitável, o processamento de dados está limitado às instalações da organização e registos são criados para cada atividade relacionada com processamento de dados.

Na área de "Diferentes partes e pessoas envolvidas na operação de processamento" a probabilidade de ocorrência é médio, pois os funcionários nos Recursos Humanos não recebem treino sobre segurança de informação e não há certezas que dados pessoais são processados e/ou destruídos de forma segura.

Na área de "Setor comercial e escala do processamento" a probabilidade de ocorrência é baixo, pois o setor de negócios de uma PME não é considerado como propenso a ciberataques.

Assume-se que não houve violação de dados pessoais no passado e que operações relacionadas com processamento de dados esteja limitada a funcionários da PME.

Baseado na avaliação referida em cima, a pontuação que a PME obtém é de 5, o que torna a probabilidade de ocorrência de ameaças ser baixa.

Avaliação de risco e adoção de medidas de segurança

A área que mais padece com falhas será aquela que gere e trata os dados pessoais dos trabalhadores, sendo que não existe políticas especificas nem treino que esclareçam as práticas seguras para o tratamento/gestão/destruição de dados, como tal é uma área com maiores problemas.

Com base no anexo A.2, e escolhendo medidas essenciais para resolução do problema, as medidas identificadas como A.3, G.3, J.2 e S.3 seriam o suficiente para mitigar o risco de perda de confidencialidade. As referências em cima são alusivas aos seguintes procedimentos:

- A.3 – A organização deverá manter um documento à parte dedicado a política de segurança no que diz respeito ao processamento a dados pessoais. Esta política deve ser aprovada e comunicada a todos os trabalhadores.
- G.3 – A resposta a incidentes deve ser documentada, sendo que deve ser incluído uma lista de possíveis mitigações e uma distribuição clara de cargos.
- J.2 – A instituição deve ter treinos estruturados e regulares para o staff, incluindo programadores específicos para a introdução de novos trabalhadores.
- S.3 – Quando utilizado software que subscreve dados (normalmente programas de deleção de dados), deve ser sempre utilizada a opção de subscrever os dados múltiplas vezes (que impedirá a sua recuperação/leitura)