APSEI Trabalho 2

Alexandre nº108122, Rodrigo nº107634

1 Assigment 2 - Cybersec and privacy

- Develop and demonstrate a data acquisition and storage process and infrastructure capable of ensuring data security, data privacy, and enabling data exploration with the desired level of arbitrary detail in the future, including legal issues access by judicial entities.
- Assessment parameters
  - System technical detail
  - System capabilities/guarantees in terms of security and privacy (users, developers, administrators, entities involved, legal authorities)
  - Level of accuracy with security, privacy and judicial access issues
  - Presentation (and video) quality
- Assessment method
  - Video up to 10 minutes demonstrating/describing the system
  - Presentation of 10min + 5min of questions
  - Presentation Handouts
- Deadline
  - Video - until April 1st
  - Presentation - during the TWO classes on April 4th

2 Email

- Notem que:
  - Vocês têm de idealizar um sistema de dados, não um serviço ou aplicação
  - Uma vez que este tipo de sistema é potencialmente muito abstrato (estamos a falar de um sistema que seja capaz de armazenar qualquer tipo de dados (p.ex. um sistema tipo Oracle ou Amazon em termos de storage), vocês podem escolher centrar o trabalho num determinado contexto, sejam os dados de uma aplicação ou os dados de um serviço
  - Se preferirem ir nessa direção (que implica simplificar o trabalho), então podem escolher qualquer ambiente em que os dados sejam grandes (i.e. pensem em maior que teradata) e que tenham regulamentação complexa (i.e. podem ter que ser disponibilizados por questões legais). Mas é o aspeto de tratamento de dados que deve ser o foco, não a aplicação/serviço
  - A complexidade final da resposta é parte da avaliação (e.g. ambientes federados, reguladores, auditores)
  - O foco do vosso trabalho deve ser sempre um sistema de dados a ser construido de forma a garantir todos os aspetos regulamentares de tratamento de informação. O trabalho tem de conter a descrição técnica e em termos de processos de uso de um sistema de armazenamento. E mostrar como os diferentes aspetos tecnicos são relacionados com aspetos de requisitos.

3 Notas tiradas na Aula

- Ideias
  - Não fazer de coisas de saúde
  - Dropbox
  - Download Jogos, Filmes, Músicas
- Video
  - Poder ser Webcam a explicar
  - Pode ser Apresentação
  - Pode ser para Empresa
- Conclusão
  - Semelhante a Dropbox
  - Dependendo de como correr o resto, video de Empresa, ou video apresentação na rua

4 Video

4.1 Introdução

Olá, o meu nome é Alexandre e hoje venho-vos falar sobre o nosso serviço SkyVault.

O SkyVault é um serviço de armazenamento de dados online, em cloud, direcionado a pessoas individuais que querem guardar os seus ficheiros remotamente de forma segura.

Cada utilizador registado tem acesso a um Vault, cujo tamanho depende do plano escolhido. Na versão grátis, têm acesso a 2GB de espaço, e nas versões acima o espaço aumenta para 2.5TB e 4TB, respetivamente.

Em qualquer versão, o utilizador tem a opção de tornar o seu Vault público para que outras pessoas consigam visualizar e descarregar o conteúdo nele contido.

A nossa prioridade é garantir a segurança e privacidade dos dados dos nossos clientes, adotando medidas robustas para proteger as suas informações de forma contínua. Ao mesmo tempo, valorizamos a simplicidade e esforçamo-nos para fornecer uma experiência fácil e acessível para todos os utilizadores.

4.2 Infraestrutura e Segurança

Olá, eu sou o Rodrigo e agora vou-vos falar sobre a arquitetura do nosso serviço SkyVault. O SkyVault é um serviço distribuído em nuvem, projetado para oferecer simplicidade, segurança e privacidade.

Acerca do armazenamento dos dados, nestes , as informações básicas dos usuários são mantidas em armazenamento discreto, servindo como índices para os dados das contas. Enquanto, os metadados dos arquivos são armazenados em serviços protegidos de banco de dados MySQL.

Sobre a sua segurança, os servidores processam os arquivos e dividem-nos em blocos. Criptografam cada bloco de arquivos usando uma cifra forte e sincronizando somente blocos que foram modificados entre as revisões, tal como podem visualizar na imagem que vai aparecer. É utilizada criptografia AES de 256 bits para garantir a segurança dos arquivos em repouso e para proteger os dados em trânsito entre os aplicativos e os servidores implementamos SSL/TLS.

É oferecida também aos nossos clientes a autenticação de dois fatores para uma camada extra de segurança no acesso às suas contas.

Agora sobre segurança fisica, os nossos data centers possuem medidas robustas de segurança, incluindo autenticação biométrica e vigilância 24/7. Contamos também com redundância geográfica

para garantir a disponibilidade contínua dos serviços, mesmo em caso de falhas em um local específico.

Toda a nossa equipe recebe treinamento periódico em medidas de segurança, incluindo conscientização sobre phishing e cuidados com informações pessoais.

4.3 Políticas

Os utilizadores, para acederem ao SkyVault, necessitam de se registar na plataforma web. Ao fazerem este registo, é-lhes pedido o seu consentimento referente às políticas de uso que estão descritas no nosso acordo de Termos de Serviço.

Neste acordo abrange vários tópicos, dos quais destacamos dois: a política de uso aceitável e a política de privacidade.

4.3.1 Política de Uso Aceitável

A nossa Política de Uso Aceitável descreve um conjunto de regras que cada utilizador tem de cumprir se quiser usufruir do nosso serviço.

Para exemplificar, o utilizador não deve:

- Explorar vulnerabilidades do nosso sistema
- Interferir com a disponibilidade do nosso serviço, através de, por exemplo, vírus, overloading ou outras ações semelhantes
- Publicar, partilhar ou armazenar conteúdo ilícito
- Utilizar os nossos serviços como suporte para serviços cloud do próprio
- Quebrar qualquer lei, incluindo armazenar conteúdo que infringe direitos à propriedade intelectual

A violação desta política pode resultar na suspensão ou término da conta do utilizador responsável.

4.3.2 Política de Privacidade

Idade de Consentimento Digital Em acordo com o GDPR, a idade mínima para consentir ao tratamento de dados digitais e utilizar o nosso serviço é 16 anos, no entanto aplica-se a idade mínima regente no país em que o utilizador reside.

Categorias de Dados Recolhidos Os dados recolhidos pelo SkyVault caem em duas categorias: informação da conta e ficheiros do Vault.

Direitos ARCO Em ambas os casos, os utilizadores, como titulares dos dados, retêm os direitos ARCO descritos pelo GDPR, ou seja, têm o direito de aceder, retificar, cancelar e objetificar o tratamento dos seus dados pessoais, sempre que o acharem que devem fazer.

Dados da Conta Os dados associados a cada conta são fornecidos pelo utilizador em três momentos: no registo, na compra de versões pagas e na configuração de autenticação por dois fatores, e são guardados o nome, email, dados de pagamento no caso de compras e número de telemóvel, como segundo fator.

Para além disso, também recolhemos dados relativos ao uso do serviço, como o espaço ocupado e a frequência de utilização, para recomendar versões do serviço que melhorem a experiência do utilizador.

Dados do Vault - DPA Por outro lado, os dados que o utilizador escolhe guardar no seu Vault requerem um cuidado especial, começando pelo estabelecimento de um DPA, ou Acordo de Processamento de Dados, entre o cliente e o SkyVault, de forma a definir os requirimentos técnicos sobre o processo de tratamento de dados por nossa parte.

Terceiros Este tipo de acordo também é realizado entre o SkyVault e empresas terceiras, que nos fornecem serviços como atendimento ao cliente e suporte técnico.

Deveres do Utilizador Continuando no tópico do cofre pessoal, o utilizador também tem deveres a cumprir relativamente aos dados que escolhe guardar. De forma resumida, o utilizador não deve armazenar conteúdos ilegais, conceito este que está descrito em detalhe no RSD, ou Regulamento de Serviços Digitais.

Conteúdos Ilegais Para garantir a deteção eficaz desse tipo de conteúdo, utilizamos um sistema automático de deteção que identifica possíveis ocorrências. Além disso, contamos com uma ferramenta de sinalização manual, que permite aos utilizadores colaborarem connosco na identificação e denúncia desses conteúdos.

Uma vez sinalizado este conteúdo, tomamos medidas imediatas para desabilitar o seu acesso e, se acharmos adequado, punir as contas responsáveis pela sua distribuição, podendo resultar no seu término. (Em casos de conteúdo ligado ao abuso de menores, informamos as entidades legais apropriadas, nomeadamente a NCMEC. (meter isto no relatório extra))

5 Planeamento Apresentação

5.1 Introdução

- Apresentações
- Falar do serviço, mencionar que é um sistema de armazenamento de dados em cloud
- Explicar porque é que escolhemos este tipo de serviço como objeto de estudo

5.2 Vídeo

- Não mostramos o vídeo, apenas uma ou duas frames que achemos relevante
- Mencionar o objetivo do vídeo promocional, explicar o que foi falado no vídeo
- Enumerar o que vamos falar ao longo do resto da apresentação

5.3 Infraestrutura

- Apresentar os topicos igual
- Reduzir info em alguns pontos e tocar em coisas que nao falei no video noutros pontos
- Dados basicos sao os dados de conta de utilizador
- Dados de arquivos pode conter informações sensiveis e por isso temos esse cuidado extra

5.4 Política de Privacidade

- Dados da conta mete-se na Infraestrutura
- DPA ? e Terceiros dentro de DPA
- RSD ? e Conteudo Legais dentro de deveres de utilizador
- Topico Acessos Judiciais / Transparência

6 Apresentação

6.1 Introdução

Bom dia, o meu nome é Alexandre, este é o meu colega Rodrigo, e hoje viémos falar sobre o serviço que criámos para este trabalho, o qual chamámos SkyVault.

O SkyVault é um serviço de armazenamento de dados online, em cloud, direcionado a pessoas individuais que querem guardar os seus ficheiros remotamente de forma segura.

Cada utilizador registado tem acesso a um Vault e existem 3 planos no total, incluíndo uma versão grátis. Para além do armazenamento de dados, o outro feature principal do nosso serviço é a possibilidade de tornar este cofre público, podendo outras pessoas aceder ao seu conteúdo.

O nosso foco no desenvolvimento deste serviço foi garantir a segurança e privacidade de dados pessoais, e garantir que os nossos utilizadores podessem exercer os direitos de proteção de dados atribuídos pela lei.

Antes de avançarmos, queria falar um pouco da razão por termos escolhido este tipo de serviço. Se nós olharmos para os produtos que estão agora no mercado, como o Dropbox e a Google Drive, conseguimos ver bem a escala da quantidade de dados armazenados, estando na ordem dos Exabytes, que corresponde a 1 milhão de Terabytes.

6.2 Video

Falando agora do vídeo, portanto, o que submetemos foi um vídeo promocional direcionado a possíveis clientes, com o objetivo de os convencer a utilizar o nosso produto e também ao mesmo tempo informá-los sobre algumas políticas relacionadas com os nossos termos de serviço, concretamente a política de uso aceitável e a política de privacidade.

Com esta apresentação, pretendemos aprofundar as medidas que temos em vigor para cumprir as leis de proteção de dados. Iremos falar novamente sobre a nossa infraestrutura, e revelar mais detalhes sobre como garantimos a segurança dos dados. Depois disso, vamos virar o nosso foco para a privacidade, e falaremos sobre algumas funcionalidades do nosso serviço que estão relacionadas com esse tópico.

6.3 Infraestrutura e Segurança

Agora sobre a arquitetura do nosso serviço SkyVault. O SkyVault é um serviço distribuído em nuvem, projetado para oferecer simplicidade, segurança e privacidade.

Acerca do armazenamento dos dados recolhidos pelo SkyVault, estes caem em duas categorias: informação da conta e ficheiros do Vault. Para além disso, também recolhemos dados relativos ao uso do serviço, como o espaço ocupado e a frequência de utilização, para recomendar versões do serviço que melhorem a experiência do utilizador.

Os dados associados a cada conta são fornecidos pelo utilizador em três momentos: no registo, na compra de versões pagas e na configuração de autenticação por dois fatores, e são guardados o nome, email, dados de pagamento no caso de compras e número de telemóvel, como segundo fator.

As informações básicas dos usuários são mantidas em armazenamento discreto, servindo como índices para os dados das contas. Enquanto, os metadados dos arquivos são armazenados em serviços protegidos de banco de dados MySQL.

Sobre a sua segurança, os servidores processam os arquivos e dividem-nos em blocos. Criptografam cada bloco de arquivos usando uma cifra forte e sincronizando somente blocos que foram modificados entre as revisões, tal como podem visualizar na imagem que vai aparecer. É utilizada criptografia AES de 256 bits para garantir a segurança dos arquivos em repouso e para proteger os dados em trânsito entre os aplicativos e os servidores implementamos SSL/TLS em conjunto com AES de 128 bits.

Agora sobre segurança fisica, os nossos data centers possuem medidas robustas de segurança, incluindo autenticação biométrica e vigilância 24/7. Contamos também com redundância geográfica para garantir a disponibilidade contínua dos serviços, mesmo em caso de falhas em um local específico.

Toda a nossa equipe recebe treinamento periódico em medidas de segurança, incluindo conscientização sobre phishing e cuidados com informações pessoais.

6.4 Privacidade

Introdução Vamos agora virar o nosso foco para o tópico da privacidade.

Para começar, quero falar um pouco sobre os regulamentos nos quais nos baseámos. O Regulamento Geral sobre a Proteção de Dados, ou GDPR, é um regulamento europeu que descreve um conjunto de regras a cumprir quando tratamos de dados pessoais, e que entrou em efeito em 2018.

Deste lado, temos o Regulamento dos Serviços Digitais, ou DSA, que é um regulamento europeu que se foca na transparência no tratamento de dados e na moderação de conteúdos ilegais em plataformas online. Este regulamento começou a tomar efeito em 2023.

Idade de Consentimento Digital Em acordo com o artigo 8 do GDPR, a idade mínima para consentir ao tratamento de dados digitais e utilizar o nosso serviço é 16 anos, no entanto aplica-se a idade mínima regente no país em que o utilizador reside.

Direitos ARCO A partir do momento que os utilizadores fazem o seu registo, eles podem exercer os direitos ARCO descritos pelo capítulo 3 do GDPR, ou seja, têm o direito ao acesso, retificação, cancelamento/esquecimento e objetificação do tratamento dos seus dados pessoais, sempre que o acharem que devem fazer.

Dados do Vault - DPA Os dados que o utilizador escolhe guardar no seu Vault requerem um cuidado especial, que começa pelo estabelecimento de um DPA, ou Acordo de Processamento de Dados, entre o cliente e o SkyVault. Um DPA é um acordo entre um controlador de dados, neste caso o utilizador, e um processador de dados, no caso nós, SkyVault, que regula e estabelece limites no processo de tratamento de dados por parte do processador. Detalhes sobre o que deve constar neste acordo podem ser encontrados no capítulo 4 do GDPR, artigos 24-43. Este tipo de acordo também é realizado entre o SkyVault e empresas terceiras, que nos fornecem serviços como atendimento ao cliente e suporte técnico.

Transparência Agora vou falar um bocado acerca da transparência no tratamento de dados.

Comecemos pelas entidades que podem aceder aos dados pessoais do utilizador. Para além das empresas terceiras com as quais estabelecemos DPAs, a staff do SkyVault também poderá aceder a estes dados no caso de:

- Serem legalmente obrigados a fazê-lo
- Ser necessário para garantir que o nosso serviço está funcional, no caso de debugging de problemas de performance por exemplo
- Ser necessário para o cumprimento dos nossos Termos de Serviço

Da mesma forma, nós estamos sujeitos a receber pedidos de acesso a dados de utilizadores por parte de entidades federais ou governamentais.

Nestes casos, é feita uma análise detalhada do pedido, por um lado para verificar se cumpre todos os requisitos legais mas também para determinar se o pedido não é muito abrangente ou desnecessáriamente invasivo, e se for, tentamos resistir dentro do possível.

Se o pedido for válido, cooperamos com essas entidades, mas só partilhamos conteúdo se tiverem um mandato de busca ou se houver uma investigação de segurança nacional pendente.

Quando ocorrem estes acessos a dados, nós notificamos o utilizador envolvido, menos em casos onde somos legalmente proibidos de o fazer, em situações de ordens de não divulgação. No entanto, assim que estas ordens expiram, nós informamos os utilizadores acerca da situação.

Por fim, de forma a cumprir o estabelecido no artigo 15 do DSA, a cada 6 meses publicamos um relatório que ilustra a moderação de conteúdo realizada nesse período de tempo, que incluí os pedidos de acesso mencionados, bem como dados relacionados com a moderação de conteúdo ilegal.

Deveres do Utilizador Continuando no tópico do cofre pessoal, o utilizador também tem deveres a cumprir relativamente aos dados que o mesmo escolhe guardar. O utilizador não deve armazenar conteúdos ilegais, Conceito este que está descrito em detalhe no Regulamento de Serviços Digitais. Este Conceito abrange uma ampla gama de situações, incluindo discursos de ódio, compartilhamento não consensual de imagens privadas, uso não autorizado de material protegido por direitos autorais, entre outros.

Legalidade no Armazenamento de Conteúdo Ilegal - SkyVault Como está descrito no artigo 6 do Regulamento de Serviços Digitais, nós não somos legalmente responsáveis pelo armazenamento deste tipo de conteúdo sendo que não temos conhecimento do que os utilizadores guardam no seu Vault. Se obtivermos esse conhecimento, tomamos a ação de remover ou desabilitar o acesso a esse conteúdo, e mais tarde punir devidamente os responsáveis.

Deteção de Conteúdo Ilegal Para garantir a deteção eficaz desse tipo de conteúdo, utilizamos um sistema automático de deteção que identifica possíveis ocorrências. Além disso, contamos com uma ferramenta de sinalização manual, que permite aos utilizadores colaborarem connosco na identificação e denúncia desses conteúdos.

Conteúdo relacionado com Abuso de Menores Em casos de conteúdo ligado ao abuso de menores, são informadas as entidades legais apropriadas, nomeadamente a NCMEC, organização sem fins lucrativos dos Estados Unidos que ajuda a prevenir o sequestro, o abuso sexual e a exploração de crianças internacionalmente.

6.5 Referências

Aqui colocamos algumas referências que nos foram utéis no desenvolvimento deste trabalho. Obrigado pela atenção, espero que tenham gostado do nosso serviço.

https://support.google.com/drive/answer/2450387?hl=pt

https://www.dropbox.com/pt$_B R$*/business/trust/security/architecture*

https://www.dropbox.com/pt$_B R$*/business/trust/security*

https://ironcladapp.com/journal/contracts/what-is-a-data-processing-agreement-dpa/

https://www.gdprregister.eu/gdpr/data-processing-agreement-dpa/

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022R2065