Module ICT 143

Rapport du groupe 3 – Winston, Quentin, Pablo, Dylan

Table des matières

1 Lois sur les protections des données

Avec la mise en place de la RGPD au niveau européen, et la révision de la LPD au niveau suisse, une réflexion sur l'état actuel de la situation a été menée, qui amène plusieurs entreprises à se mettre à niveau en parlant de traitement des données.

1.1 LPD

La loi fédérale sur la protection des données a entrée en vigueur le 1 juillet 1993, cette dernière vise à protéger la personnalité et les droits fondamentaux des personnes qui font l'objet d'un traitement de données (LPD art1).

1.2 RGPD

L'Union Européenne représentée par son parlement a voté une Loi afin d'assurer le bon traitement des données personnelles ses citoyens, la **RGPD** (règlement général sur la protection des données). Cette dernière, entrée en vigueur le 25 mai 2018, vise à donner aux citoyens plus de contrôle sur leurs données personnelles, à responsabiliser davantage les entreprises et à renforcer le rôle des autorités de protection des données.

Première chose à se demander : Qu'est qu'une donnée personnelle ?

Toutes les informations qui se rapportent à une personne identifiée ou identifiable (art3 LPD). Par exemple : Nom et prénom, numéro de passeport, etc.

En vrai, à quoi sert ces deux lois ?

La LPD et RGPD ont été mises en place afin d'éviter la mauvaise utilisation des données de la personne, comme par exemple le profilage, vu dernièrement dans le scandale Facebook et Cambridge Analytica.

Qui est concerné ?

Toutes les entreprises, organes fédéraux ou personnes privées traitant des données personnelles d'un tiers, avec quelques exceptions, comme par exemple : LPD art2 al2a « elle ne s'applique pas aux données personnelles qu'une personne physique traite pour un usage exclusivement personnel et qu'elle ne communique pas à des tiers ; ».

1.3 Mise en conformité

Principes Juridiques (liste pas exhaustive):

Licéité, bonne foi, proportionnalité, finalité, reconnaissabilité et exactitude.

•Principe de la **bonne foi** : la collecte doit se faire dans la loyauté, de manière transparente

• Principe de la **proportionnalité** : les données doivent être aptes, objectivement nécessaires pour atteindre le but poursuivi ;

• Principe de **reconnaissabilité** : la collecte et la finalité du traitement doivent être reconnaissables pour la personne concernée ;

• Principe de **finalité** : la collecte, le traitement des données doivent se faire dans un but préalablement défini. Quid du big data ?

• Principe **d'exactitude** des données (droit de rectification)

• Principe de **sécurité** : des mesures techniques et opérationnelles doivent être prises pour protéger les données et éviter tout traitement non autorisé

1.4 Organisation et actions :

- Nommer Un DPO (Digital protection Officer), responsable par but principalement permettre à un organisme effectuant des traitements de données personnelles de s'assurer qu'il respecte bien la réglementation applicable à leur protection.
- Mentions d'informations : Les personnes concernées doivent être informées de qui est derrière la collecte, de combien de temps seront conservés les fichiers, la finalité des données collectées et les informer sur comment elles peuvent exercer leurs droits.
- Être en mesure de répondre aux sollicitations d'une personne à accéder à ses données, aussi les modifier et supprimer selon sa volonté. Par exemple la mise en place d'un formulaire de contact.
- Demander l'accord aux personnes et leur donner la possibilité de retirer cet accord.
- Mettre en place des mesures de sécurité adaptées à la sensibilité de la donnée sauvegardée. Données sensibles, exemple : ethnie ou race, religion, options sexuelles, etc.
- Analyser les fichiers et tenir un registre de traitements des données.

1.5 Mesures techniques adéquates

RGPD oblige le responsable du traitement à mettre en œuvre les mesures techniques et organisationnelles appropriées afin de garantir un niveau de sécurité adapté au risque.

Elle assure aussi l'obligation de notifier à l'autorité de contrôle les violations 72h au plus tard.

Voici une liste de mesures de sécurité à prendre :

- Sensibiliser les utilisateurs ;
- Authentifier les utilisateurs ;
- Tracer les accès et gérer les incidents ;
- Sécuriser les postes de travail ;
- Sécuriser l'informatique mobile ;
- Protéger le réseau informatique interne ;
- Sécuriser les serveurs ;
- Sécuriser les sites web ;
- Sauvegarder et prévoir la continuité d'activité ;
- Archiver de manière sécurisée ;
- Encadrer la maintenance et la destruction des données ;
- Sécuriser les échanges avec d'autres organismes ;
- Protéger les locaux ;
- Encadrer les développements informatiques ;
- Chiffrer, garantir l'intégrité ou signer.

2 Casino de Montreux

2.1 Introduction

Le casino de Montreux est le premier casino de Suisse en termes de résultat brut des jeux, il appartient au Groupe Barrière, groupe français de divertissement (hôtels, casinos, spas…). Le groupe possède deux autres casinos en Suisse : Fribourg (Granges-Paccot) et Courrendlin (Jura).

2.2 Concerné !

Le Casino de Montreux traite un nombre considérable de données, principalement en raison du Club Barrière (programme de fidélité du casino) et aussi pour des raisons juridiques, une fois que toutes les entrées sont sauvegardées par le but de prestation de comptes à la CFMJ (Commission Fédérale des maisons de jeux). Donc beaucoup de données sensibles.

2.3 Actions et mesures prises.

Le casino a formé deux DPO et nommé des responsables de traitement par secteur (exemple RH, Marketing, etc.) ainsi comme des suppléants aussi formés pour le traitement de données.

Le rôle des responsables de traitement de donnée est de tenir un registre à jour de tous les fichiers contenant des données personnelles (selon procédure mise en place par le DPO). Ensuite tout est validé par le DPO. Le DPO met en place des nouvelles mesures de traitement et sécurité, il doit aussi former les utilisateurs selon les principes juridiques et mesures de sécurité.

La sécurité des données est déjà en place avec des backups journaliers, clustering, firewall, portes sécurisées, entre autres.

3 La Loterie Romande

3.1 Introduction

Le but de la Loterie Romande est d'organiser et exploiter, avec les autorisations prescrites par la loi, des loteries et paris comportant des lots en espèces ou en nature et d'en destiner le bénéfice net à des institutions d'utilité publique – sociale, culturelle, de recherche ou sportive – profitant aux cantons romands.

3.2 Les données au sein de la Loterie Romande

La Loterie Romande traite un grand nombre de données, majoritairement en raison des jeux d'argents et des données clients que cela importe d'avoir. La société doit se plier à LPD et au RGPD car des clients Suisses ou étrangers à la Suisse peuvent aussi jouer aux jeux d'argent de la société. Toutes ces données doivent donc être gérer très sérieusement car cela représente beaucoup de données sensibles.

Nos normes standards concernant ces lois au point de vu sécurité sont toutes issues de l'ISO 27001.

3.3 Actions et mesures

3.3.1 Protections logiques

Toutes les données de la Loterie Romande sont stockées en interne dans des Datacenter. Ces données ont une rétention de 10 ans sur l'archivage. L'archivage se fait dans les serveurs de la Loterie, aucun archivage papier n'est présent.

Chaque collaborateur de la Loterie Romande doit suivre une journée d'information concernant la sécurité physique et logique lors de sa première journée de travail dans l'entreprise. Cette formation sert à instruire les collaborateurs des risques potentiels qu'ils pourraient faire et ce qu'il faut éviter.

Afin de vérifier si notre système de sécurité est fiable, nous procédons à un audit technique. Chaque moi un scan complet de nos systèmes est effectué.

3.3.2 Protections techniques

L'accès à nos sites, nos serveurs, nos Datacenter, nos armoires de câbles se font soit par l'intermédiaire de l'Active Directory soit par un système de badge et de code.

Les serveurs de productions sont répliqués de manière synchronisée sur deux Datacenter.

Pour gérer nos logs, nous possédons une grosse base de données dans laquelle tous nos logs sont répertoriés. Ces logs sont contrôlés par une autre entreprise.

Dans l'entreprise nous chiffrons tous les flux ssl et https ainsi que nos cassettes de sauvegarde.

Afin de prévenir les virus, nous avons tous un antivirus sur nos postes, un système qui vérifie tous les mails entrants et un contrôle des flux http et https.

4 VTX

4.1 Introduction

VTX est une entreprise qui occupe la télécommunication. La société a été fondée en 1989 et son nom signifie Videotex. Le siège est à Pully et nous avons d'autre succursale à Genève, Sion et Bâle.

Nous fournissons :

- Internet
- Téléphonie
- Nom de domaine
- Hébergement
- Mail
- Sécurité de réseau informatique
- Télévision
- Cloud

4.2 Les techniques utilisées

Pour conserver nos données nous utilisons comme technologie Bacula / Veam et notre hardware est du NetApp.
Le toute est conservé en VHD.

Nous enregistrons toutes les 3 semaines en bande magnétique en cas d'attaque grave via un ransomware.

Nos donnée son sécurisé physiquement par un lieu inconnu et ne sont accessible que par l'équipe qui s'occupe des backups.

Les sauvegardes se font toutes les 8 heures et son sauvegarder sur plusieurs de nos Datacenter.

En cas de récupération de nos données, nous envoyons des mails à tous nos clients via un système automatique en 48 heures. Si non avons leurs portables dans la base de données le programme leurs envoie aussi un SMS.

Ensuite VTX au niveau de la LPD et le RGPD se situe dans les entreprises ou cette protection doit s'appliqué de façons la plus rigoureuse, dû au fait qu'elle détient l'intégralité des données personnel des clients.

Nous avons par exemple des mesures ou le renouvellement de mot de passe n'est même plus visible pour les employés concernés aux bouts de 24 heures.

5 Université de Lausanne

5.1 Présentation d'entreprise

L'Université de Lausanne, bâtiment dédié aux étudiants, professeurs et chercheurs universitaires, est un bâtiment qui regroupes pas moins de 15'000 étudiants et 5'000 employés situés sur les bords du Lac Léman, et il est composé de 7 facultés : médecine-

biologie / sciences sociales / lettre / théologie / géosciences / droit / commerciales (HEC). Ce bâtiment a eu ses débuts en 1537 et l'un des plus vieilles sociétés de Suisse.

5.2 La volumétrie des données

Constitué de 28 serveurs physiques, repartit sur 3 Datacenters, on compte 550 serveurs virtuelles.

Également 2 SAN (Storage Area Network) d'environ 90 TB chacun.

5.3 Les techniques et technologies utilisés

L'Université de Lausanne a plusieurs technologies pour effectuer les sauvegardes des machines, cela dépend de quel type de machine on utilise.

Au niveau des fichiers et d'exchange, nous avons NetWorker en version 9x pour la sauvegarde. Il effectue une sauvegarde quotidienne incrémentale sauf le samedi, et effectue une sauvegarde full chaque vendredi. La rétention des fichiers est de 3 mois selon les directives de la SLA (Service Level agreement) est une rétention de la base de données de 4 semaines, il effectue une sauvegarde full de la base de données de manière quotidienne. Un Recover Point Objective (RPO) d'un maximum de 24 heures pour les fichiers et un RPO maximum de 8h pour les bases de données.

Au niveau des machines virtualisées, le logiciel Avamar est utilisé pour la sauvegarde de 150 machines virtualisés critiques. Il effectue une image de chaque VMs de manière quotidienne, sauf le samedi. La rétention des sauvegardes est de 7 jours.