

QUELLE SECURITE INFORMATIQUE POUR UNE PROTECTION RENFORCEE DES DCP

Coulibaly Nahoua

Chef du Service Protection des Données à
Caractère personnel

ARTCI

PLAN

Introduction

1. Définition (Sécurité informatique, données à caractère personnel...)
2. Enjeux des traitements des données à caractère personnel
3. Risques liés aux traitements
4. Impacts des mauvais traitements
5. Propositions de solutions

Conclusion

INTRODUCTION

- Le responsable d'un traitement de Données à Caractère Personnel (DCP) a l'obligation d'assurer un niveau de sécurité suffisant
- Nécessité d'appliquer les bonnes pratiques de sécurisation du système d'information.

1. DÉFINITIONS – *Sécurité informatique*

- La sécurité informatique se définit comme un ensemble de moyens technique, organisationnel, juridique et humain nécessaires et mis en place pour conserver, rétablir, et garantir la sécurité des systèmes informations.
- Elle est intrinsèquement liée au système d'information.

1. DÉFINITIONS - *Données à Caractère Personnel (DCP)*

- **Données informatiques ou données** : toute représentation de faits, d'informations ou de concepts sous une forme qui se prête à un traitement informatique, y compris un programme de nature à faire exécuter une fonction par un système d'information
- **La donnée** représente aujourd'hui la première richesse de toute entreprise
 - **90%** des données créées dans le monde l'ont été durant les deux dernières années *(source IBM)*
 - **+ 81%** de croissance entre 2012 et 2014 pour les données transférées via mobiles, pour atteindre 1,5 million de gigaoctets par mois. *(Source : Cisco Systems)*
- **Donnée à caractère personnel** : toute information de quelque nature qu'elle soit et indépendamment de son support, y compris le son et l'image, relative à une personne physique identifiée ou identifiable directement ou indirectement, par référence à un numéro d'identification ou à un ou plusieurs éléments spécifiques, propres à son identité physique, physiologique, génétique, psychique, culturelle, sociale ou économique.

2. ENJEUX DES TRAITEMENTS DE DCP

- Une grande partie des données que sont amenées à traiter les entreprises concernent directement les personnes (clients, utilisateurs...)
- Les étapes du traitement des données à caractère personnel :
 - Collecte / enregistrement
 - Stockage
 - Suppression

3. RISQUES LIÉS AUX TRAITEMENTS - *Faits*

- **Début 2012, société Target** : la chaîne de supermarchés américaine Target a pu déduire qu'une fille de 16 ans était enceinte et lui envoyait en suggestion publicitaire des produits pour nourrisson.
- **19 décembre 2013** : la même société Target est victime du vol de données de plus de 110 millions de clients. Ces données comprennent les données de carte bancaires avec les codes PIN mais aussi les informations personnelles des clients comme évoqué plus haut...
- **31 Aout 2014** : « **celebgate** » ! plus de **500** photos intimes de diverses stars américaines sont piratées et mises en ligne sur les réseaux sociaux **Reddit** et **Tumblr**. Le service de stockage **iCloud** d'Apple et la négligence des utilisateurs sont mis en cause

3. RISQUES LIÉS AUX TRAITEMENTS - *Détail*

- **La collecte :**
 - en cas de collecte via le Web, possibilité de récupération des données par un attaquant (écoute passive, phishing)
 - pour toute autre forme de collecte le risque est lié à la confiance de la personne concernée
- **Le stockage :** Accès frauduleux aux bases de données, peut être
 - externe (via le site web par injection SQL, XSS ou par accès au réseau de l'entreprise)
 - interne (personne non habilitée ayant obtenu frauduleusement ou non les droits d'accès)
- **La suppression :**
 - mauvaise suppression des données (récupération ultérieure des données possible)
 - mauvaise destruction des supports

4. IMPACTS DES MAUVAIS TRAITEMENTS - *Données à caractère personnel (DCP)*

L'impact des vols de données personnelles est indéniablement néfaste pour :

- **Les consommateurs** qui voient ainsi leur vie privée violée et peuvent par la suite être facilement ciblées par des personnes malhonnêtes
- **Les entreprises**, du point de vue de l'image de marque, de la perte de confiance des consommateurs, des pertes financières et surtout des sanctions législatives lorsque les dispositions suffisantes n'ont pas été prises pour la protection des données

4. IMPACT DES MAUVAIS TRAITEMENTS - *Chiffres*

Quelques chiffres pêle-mêle :

- 98% des entreprises françaises sont étroitement dépendantes des données !
- Parmi elles 80% des entreprises ferment après un sinistre informatique
- Le prix payé par les entreprises face à leurs manquements au regard de leurs législations respectives s'élèvent à :
 - 6.75 Mds € aux Etats-Unis
 - 2.58 Mds € en Allemagne
 - 1.9 Mds € en Grande Bretagne

4. IMPACT DES MAUVAIS TRAITEMENTS - *Evolution*

- D'après Symantec le nombre de vol de données est en perpétuelle évolution :
 - hausse de 62% des violations de données sensibles entre 2012 et 2013
 - Hausse de 114% des attaques par ransomware entre 2013 et 2014

5. PROPOSITIONS DE SOLUTIONS

Trio C I A classique :

- **Confidentialité** : les données ne sont uniquement accessibles qu'aux personnes autorisées
- **Intégrité** : les données ne subissent pas d'altération fortuite, illicite ou malveillante
- **Authentication** : l'identité des personnes qui accèdent aux données est vérifiée avant d'autoriser tout accès

5. PROPOSITIONS DE SOLUTIONS (UTILISATEURS) – *Collecte des données*

- Utilisation du HTTPS afin de :
 - Sécuriser les transactions et protéger les données des utilisateurs contre les écoutes
 - Permettre aux utilisateurs d'être sûrs de l'identité du site en vérifiant le certificat électronique

Fonction: confidentialité

5. PROPOSITIONS DE SOLUTIONS (UTILISATEURS) – *Collecte des données*

- Éviter de divulguer des informations ou des fichiers sensibles sur les réseaux sociaux ou des services en ligne
- Prendre conscience de la valeur des données personnelles et donc toujours vérifier l'identité des personnes à qui on les communique
- Utiliser une plateforme « TOR » lors d'échange sur la toile
- Ne pas transmettre des informations sensibles en étant connectés à des réseaux wifi publics non sécurisés

5. PROPOSITIONS DE SOLUTIONS (CAS D'ENTREPRISE) – *Stockage des données*

Sécurité physique :

- Restreindre l'accès physique aux serveurs et aux locaux de ces serveurs.

Sécurité réseau :

- Partitionner le réseau en créant des VLANs
- Installer des serveurs Proxy
- Séparer les équipements sensibles du reste du réseau (intranet-DMZ etc.)
- Configuration (pare-feu, IDS etc.)

Sécurité logicielle :

- Configurer les droits, accès et habilitations des utilisateurs afin que seules les personnes autorisées et nécessaires accèdent aux données
- Se prémunir des failles applicatives (mises à jour régulières et patches) et des failles web (injections SQL, XSS) qui sont les moyens les plus courants de vols des données
- Installer un outil de suivi et d'analyse des logs

En cas de stockage dans le Cloud vérifier la législation en vigueur dans le pays concerné et les conditions d'utilisation du service

Fonctions :
*confidentialité,
intégrité,
authentification*

5. PROPOSITIONS DE SOLUTIONS (CAS D'ENTREPRISE) - *Suppression des données*

- Utiliser des techniques d'effacement sécurisé (basées sur un nombre de passes élevé). Plusieurs normes existent (NIST SP-800-88, British HMG Infosec Standard 5, Enhanced Standard)
- En cas de renouvellement des supports de stockage, procéder à une destruction physique ou magnétique de ces supports.
- Adopter les normes ISO 2700X relative à la sécurité du système d'information.

Fonctions: confidentialité, intégrité

CONCLUSION

- Le traitement des DCP nécessite de prendre beaucoup de précautions tant au niveau légal que technique, et sur ce point il est primordial d'appliquer les règles de bonnes pratiques en matière de sécurité informatique.



MERCI

REFERENCES

- <http://www.digital-insurance.me/10-chiffres-cles-du-big-data/>
- <http://virrea.fr/fr/securite-statistiques>
- <http://www.lemondeinformatique.fr/actualites/lire-hausse-de-113-des-attaques-par-ransomware-en-2014-60891.html>