Sécurité de l'information

PROTECTION DES DONNÉES PERSONNELLES

UNIVERSITÉ DE STRASBOURG

Sommaire

- Session 1
  - Les critères de sécurité de l'information
  - La vie privée
  - Les acteurs
  - Les enjeux
  - Les textes
- Session 2
  - Menaces et risques
  - Différents scénarii et exemples
  - En entreprise
- Session 3
  - Le paramétrage des outils
  - RGPD
  - Bonnes pratiques (ISO 27002)

Sécurité de l'information

Les critères

- Disponibilité

  Perte, vol, suppression, accès impossible

- Intégrité

  Modification, altération, falsification

- Confidentialité

  Divulgation

- Auditabilité

  Absences de traces et/ou de preuves

La vie privée, c’est quoi ?

Définition ?

- Vie privée ≠ vie publique
- Subjectivité
- Culture
- Droit au respect de la vie privée inscrit dans la législation

Les données personnelles

Toute donnée ou information permettant, directement ou indirectement, d'identifier une personne physique et essentiellement relative à :

- Son identité
- Son mode de vie, ses opinions politiques, religieuses, philosophiques
- Son image
- Son état de santé
- Sa situation familiale, financière, professionnelle, judiciaire
- Ses déplacements

Les acteurs

- Fournisseurs d'accès et gestionnaires réseau
- Propriétaires et gestionnaires de datacenters, GAFAM
- Fabricants matériels et logiciels
- Entreprises
- États, UE, institutions (Défense nationale, CNIL, Anssi…)
- Pirates, hackers…
- Réseaux « sociaux »
- Vous !!!

Les enjeux

- Vie privée ≠ vie publique ≠ vie professionnelle
- E-réputation (recrutement, diffamation, harcèlement, intox…)
- Usurpation d'identité
- Collecte de données, constitution de bases et leur utilisation, profilage
- Nécessité, pour les utilisateurs, de développer une « culture » de la sécurité de l'information
- Vides et retards juridiques

Les principaux textes

- Code pénal
- Code civil
- Code de la propriété industrielle et intellectuelle
- Code des Postes et des communications électroniques
- Code du travail
- Code de la consommation
- RGPD et sa retranscription par la CNIL
- Extra territorialisation du droit étatsunien

Sécurité de l'information

PROTECTION DES DONNÉES PERSONNELLES

UNIVERSITÉ DE STRASBOURG

Sommaire

- Session 1
  - Les critères de sécurité de l'information
  - La vie privée
  - Les acteurs
  - Les enjeux
  - Les textes
- Session 2
  - Menaces et risques
  - Différents scénarii et exemples
  - En entreprise
- Session 3
  - Le paramétrage des outils
  - RGPD
  - Bonnes pratiques (ISO 27002)

Classification de l'information

Quelles informations protéger ?

- Besoins en disponibilité
- Niveau de confidentialité
- Protection de l'intégrité

Quel impact en cas de

- Non disponibilité
- Divulgation
- Modification accidentelle ou malveillante

Classification des données personnelles

Recensement des documents et informations

- Courriers, données bancaires, commerciales et fiscales
- Photos
- État civil, santé, famille
- Documents de travail
- Réseaux sociaux …

Définir les éléments essentiels à protéger en fonction de

- Besoins de sécurité
- Méthodes d'attaque, scénarios de risque
- Opportunité
- Gravité

Quel évènement redoutez-vous ?

Menace (ou danger)

- Acte ou événement pouvant entraîner un impact négatif sur le système d'information ou sur l'activité supportée par celui-ci

Risque

- Scénario combinant un événement redouté et un ou plusieurs scénarios de menaces
  - Impact ou gravité (pertes engendrées)
  - Probabilité de survenance (ou opportunité)
  - Acceptabilité et notion de risque résiduel

Prévoir le pire, toujours…

Exemples de menaces

- Vols de matériel et/ou de données
- Mise au rebut
- Piratages (Intrusion, hameçonnage, rançon après cryptage, virus…)
- Panne matérielle ou logicielle
- Catastrophe naturelle…

Exemples d’impacts

- Perte d’image, e-réputation
- Pertes financières
- Reconstruction des données

En entreprise

Gouvernance de la sécurité de l'information

- Le chef d'entreprise est seul responsable des traitements
- Le responsable SSI est sous l'autorité directe du chef d'entreprise
- La SSI est pilotée et évaluée (plan d'actions et audits)
- Le personnel doit être sensibilisé, voire formé
- Il est recommandé d'établir et de diffuser une charte d'utilisation des outils et moyens numériques
- Mise en place d'une cartographie des risques par processus
- Intégration de la SSI dans les projets et leur évolution

En entreprise

Les textes

- Le contrat de travail
  - Lien de subordination
  - Secret professionnel
  - Clause de loyauté et de non-concurrence
- Le code du travail
- Le code de la propriété industrielle et intellectuelle

En entreprise

Un grand principe : le « besoin d'en connaître »

Gestion des accès à l'information

- A chacun son métier
- A chacun ses compétences
- A chacun ses données

Journalisation des accès

Horodatage et certification des documents (création et modifications)

En entreprise

Le Plan de continuité d'activité (PCA)

Le PCA a pour objet de réduire les conséquences d'évènements désastreux à caractère exceptionnel et de favoriser le retour à un fonctionnement normal ou dégradé.

A partir de l'identification des risques, des scénarios possibles et probables, et des besoins de continuité, mise en place de procédures organisant :

- L'alerte
- La gestion de crise
- Les tests
- Le maintien du PCA en condition opérationnelle

Merci pour votre attention

Rendez-vous le 2 avril pour notre séance

« RGPD et bonnes pratiques »

Sécurité de l'information

PROTECTION DES DONNÉES PERSONNELLES

UNIVERSITÉ DE STRASBOURG

Sommaire

- Session 1
  - Les critères de sécurité de l'information
  - La vie privée
  - Les acteurs
  - Les enjeux
  - Les textes
- Session 2
  - Menaces et risques
  - Différents scénarii et exemples
  - En entreprise
- Session 3
  - RGPD
  - Le paramétrage des outils
  - Bonnes pratiques (ISO 27002)

RGPD

Champs d'application

Le règlement s'applique aux traitements de données personnelles automatisés en tout ou partie ainsi qu'aux fichiers non automatisés.

Il s'applique aux responsables de traitement ainsi qu'aux sous-traitants ayant un établissement dans l'UE, indépendamment du lieu d'exécution du traitement.

Il s'applique également aux traitements visant des personnes de l'UE pour des offres de biens ou services au sein de l'UE.

Un responsable de traitement établi hors UE devra désigner un représentant.

RGPD

Ce qui ne change pas

Les principes concernant les données (pertinentes, limitées, respect de la finalité du traitement, durée de conservation…)

Les données dites « sensibles »

Les principes de licéité des traitements

Les droits des personnes concernées

Les missions des autorités de régulation (CNIL)

L'obligation de sécurité de l'information

L'encadrement des transferts de données hors de l'UE

Certaines particularités peuvent faire l'objet de lois nationales

RGPD

Ce qui change

L'élargissement du champ territorial à tous les responsables de traitement

La portabilité des données

Les formalités préalables sont remplacées par une obligation de preuve de conformité

L'instauration d'une responsabilité du sous-traitant

La notification obligatoire des incidents et failles de sécurité

Le consentement des mineurs (16 ans en France)

Le renforcement des sanctions

La possibilité de lancer des actions de groupe

La persistance de dispositions nationales

RGPD

Droits des personnes

Droit :

- D'accès
- De rectification, de mise à jour
- D'opposition
- A l'oubli
- Au déréférencement (ne plus apparaître dans les moteurs de recherche)
- A l'effacement (suppression des supports physiques)
- A l'image
- Portabilité

RGPD

Jurisprudences…

Moyens de recueil et preuve du consentement

- Un « like » suffit-il ?

Données personnelles et privées en entreprise

- Renommer les mails, fichiers et dossiers avec la mention « privé »
- L'employeur peut accéder aux outils informatiques mis à disposition de ses salariés et donc à leurs fichiers et correspondances, mais ne doit en aucun cas porter atteinte à leur vie privée de façon déloyale et disproportionnée (divulgation, diffamation…)

Testament numérique

- Toute personne peut donner ou enregistrer des directives sur la communication de ses données personnelles après son décès

SSI Bonnes pratiques

Paramétrage

Paramétrage des outils (PC, Tablette, Smartphone)

- Dans les menus respectifs de paramétrage, désactiver :
  - Caméra, micro, localisation
  - L'autorisation donnée à certaines applications d'accéder à certaines de vos données comme les contacts, la messagerie, les agendas

N'activer ces options qu'en cas de besoin, par exemple micro et caméra lors d'une session Skype.

SSI Bonnes pratiques

Logiciels

Garder la main !

Installer un antivirus et le maintenir à jour

Maintenir à jour le système d'exploitation

Disposer d'un support de restauration du système d'exploitation

Créer des points de restauration

Utiliser les options de configuration des applications

Tenir un « livre de bord » des incidents, installations, désinstallations et mises à jour d'applications

En cas de téléchargement de logiciel :

- Se renseigner sur la fiabilité du site fournisseur
- Procéder à une analyse antivirale du fichier téléchargé avant de l'exécuter

SSI Bonnes pratiques

Matériels

Bien que ne possédant que très peu de pièces mécaniques, les outils restent fragiles :

- Pas de chocs, chutes ou secousses

Autres menaces principales :

- Les champs magnétiques
- La chaleur
- La poussière

Pensez à vos données avant

de mettre votre matériel au rebut

SSI Bonnes pratiques

Données

Classifier les données (publiables, internes ou à diffusion restreinte, confidentielles…)

Séparer le personnel du professionnel

Effectuer des sauvegardes régulières (les clés USB ne servent qu'au transport, pas à la sauvegarde)

Créer autant de comptes que d'utilisateurs de l'outil

Créer un espace crypté sur le disque pour les données sensibles

Protéger certains fichiers par mot de passe si l'application le permet

Ne pas activer le partage d'unité (C:\, D:\…) ou de dossiers

Vider la corbeille en fin de session

SSI Bonnes pratiques

Adopter une méthode de création et de gestion des mots de passe :

- Ne jamais utiliser un même mot de passe pour toutes les applications ou utilisations
- Un mot de passe fort doit être constitué d'au moins 12 lettres, majuscules et minuscules, chiffres, caractères spéciaux
- Changer régulièrement ses mots de passe
- Un mot de passe doit être facile à retenir et difficile à deviner
- Ne pas y inclure des éléments personnels ou familiaux
- Utiliser une application de gestion de mots de passe
- Un mot de passe est confidentiel par nature

SSI Bonnes pratiques

Réseaux

Désactiver l'accès WIFI si non nécessaire à l'activité

Ne pas accepter une connexion WIFI non sécurisée (sans mot de passe)

Utiliser une connexion VPN en fonction de l'enjeu et ne transmettre que des fichiers cryptés ou compressés avec mot de passe

Utiliser les options de configuration de votre navigateur

Vérifier la sécurisation d'un site (HTTPS://) + cadenas

Accepter éventuellement les cookies mais paramétrer le navigateur pour leur suppression à la fermeture de la session

Ne jamais accepter la proposition « enregistrer le mot de passe »

Vérifier les partages de dossiers à l'aide de l'explorateur de fichiers

SSI Bonnes pratiques

Messagerie

Classifier les mails de la même manière que toutes vos informations

Enregistrer les pièces jointes si besoin et les supprimer de la messagerie

Sauvegarder régulièrement mails et carnet d'adresses

Vider les corbeilles

Ne pas se « jeter » sur sa boîte de réception, faire des contrôles de vraisemblance lors de la réception :

- Expéditeur inconnu
- Contexte
- Vérification des liens en background des boutons et options, de la qualité orthographique ou grammaticale, de la qualité des objets graphiques…

Ne pas enregistrer les mots de passe (« voulez-vous mémoriser… »)

SSI Bonnes pratiques

Réseaux sociaux

En ce moment, j' essaie de me faire des amis en dehors de Facebook, tout en appliquant les mêmes principes.

Alors tous les jours, je descends dans la rue et j' explique aux passants :

Ce que j' ai fait la veille,
Ce que j' ai mangé,
Comment je me sens,
Ce que je suis en train de faire,
Ce que je vais faire demain,

Je leur donne des photos de ma femme, de mes enfants, du chien, de moi en train de laver ma voiture, et de ma femme en train de coudre.
J' écoute aussi les conversations des gens et je leur dis « j' aime ! »

Et ça marche ! Actuellement j' ai déjà 4 personnes qui me suivent : 2 policiers , un psychiatre et un psychologue.

SSI Bonnes pratiques

Réseaux sociaux

Avant tout, configurer les paramètres Sécurité et/ou Confidentialité

Opter pour une diffusion restreinte de vos publications, publier vous engage

Hors réseaux professionnels et associatifs, il n'y a aucun intérêt à avoir des centaines de relations

N'inviter que des personnes déjà connues

Ne pas accepter a priori d'invitation de personnes inconnues, même s'il s'agit d'amis d'amis

Votre vie privée ne regarde que vous et vos proches

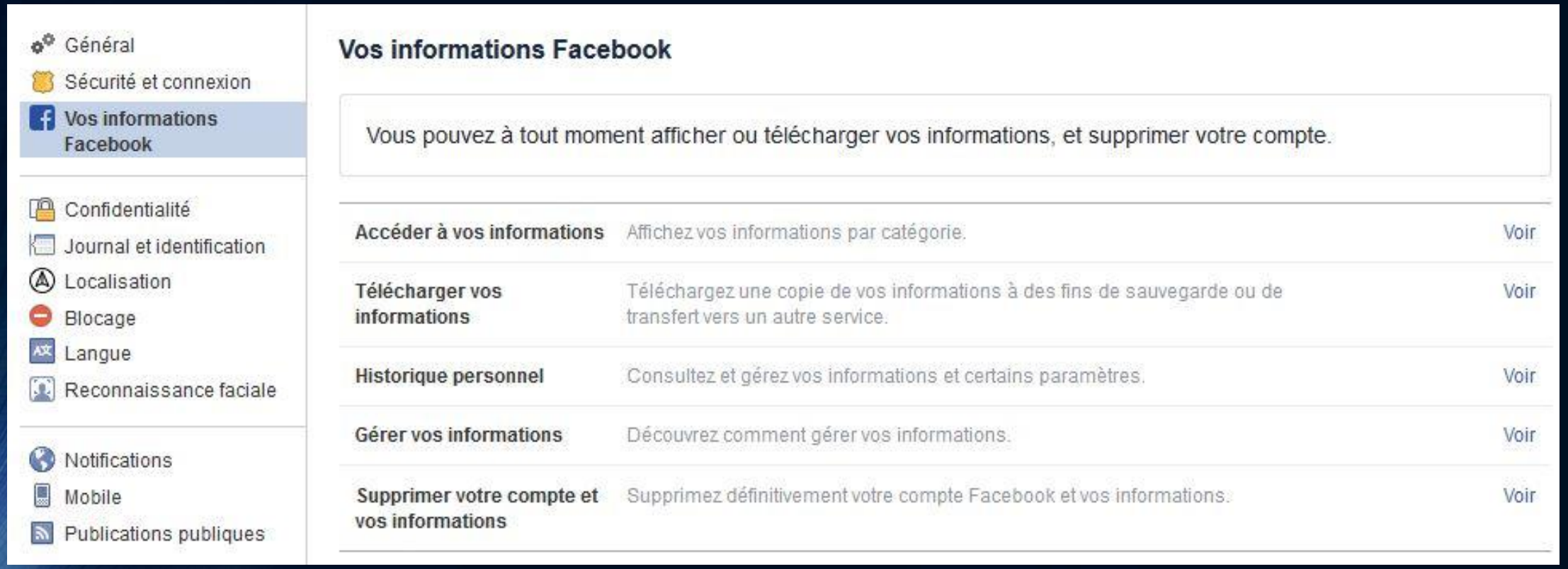
Prendre du recul en téléchargeant régulièrement ses informations

SSI Bonnes pratiques

Réseaux sociaux

SSI Bonnes pratiques

Réseaux sociaux



Merci pour votre attention

Je reste à votre écoute

reflexe.ssi@orange.fr