SEANCE TD SÉCURITÉ INFORMATIQUE (DURÉE 45 MN)

Objectifs :
— connaître la différence entre identification et authentification (dont à 2 facteurs)
— sécuriser son espace de travail local et distant et ses données (personnelles et professionnelles)
— se protéger de la perte de données, de la malveillance et des nuisances d'Internet
— protéger la confidentialité de ses communications
— détecter un comportement anormal de votre environnement matériel et logiciel afin de déceler la présence d'un virus, d'un logiciel malveillant…
— évaluer le niveau d'un risque informatique et de le traiter
— maîtriser ses traces et son identité numérique /e-reputation sur Internet
— protéger ses données contre la collecte massive et son exploitation (Big Data)
— respecter et protéger les données des autres

PIX : Domaine 4. Protection et sécurité

4.1. Sécuriser l'environnement numérique

Sécuriser les équipements, les communications et les données pour se prémunir contre les attaques, pièges, désagréments et incidents susceptibles de nuire au bon fonctionnement des matériels, logiciels, sites internet, et de compromettre les transactions et les données (avec des logiciels de protection, des techniques de chiffrement, la maîtrise de bonnes pratiques, etc.).

THÉMATIQUES ASSOCIÉES

Attaques et menaces ; Chiffrement ; Logiciels de prévention et de protection ; Authentification ; Sécurité du système d'information ; Vie privée et confidentialité

4.2. Protéger les données personnelles et la vie privée

Maîtriser ses traces et gérer les données personnelles pour protéger sa vie privée et celle des autres, et adopter une pratique éclairée (avec le paramétrage des paramètres de confidentialité, la surveillance régulière de ses traces par des alertes ou autres outils, etc.).

THÉMATIQUES ASSOCIÉES

Données personnelles et loi ; Traces ; Vie privée et confidentialité ; Collecte et exploitation de données massives

(4.3 Traitée en exposés)

Bibliographie/webographie :

- Fiche de cours [pix_securite]
- Livres et articles sur la sécurité informatique, l'identité numérique, les Big Data, à la BU via le moteur de recherche interne Focus *(limiter via la recherche avancée à BU Orsay = BU Sciences)* : https://www.bibliotheques.universite-paris-saclay.fr/
- Les articles de Wikipedia sur les différentes notions.
- Sites de référence :
  CNIL http://cnil.fr
  ANSSI (Agence Nationale de Sécurité des Systèmes d'Information), rubrique particuliers.
  https://www.ssi.gouv.fr/particulier
  Infographies de l'ANSSI :
  https://www.ssi.gouv.fr/particulier/precautions-elementaires/infographies-2/
  Site recensant les canulars/fake news : http://hoaxbuster.com

- Chiffrer ses mails de bout en bout
  Protonmail https://proton.me/fr/mail https://proton.me/fr/mail/security
  explications pour une utilisation avancée du chiffrement : https://emailselfdefense.fsf.org/fr/

Travail préalable :

1. Face aux dangers que l'informatique peut faire peser sur les libertés, quelle autorité en France est chargée de protéger la vie privée ainsi que les libertés individuelles et publiques ?
2. Quel texte législatif de l'U.E. vise à protéger les données personnelles des citoyens européens ? (il s'applique aussi aux plateformes américaines telles celles des GAFAM…)
3. Qu'appelle-t-on donnée personnelle ? Donnée sensible ? Cf https://cnil.fr
4. Si besoin : vérifiez que vous connaissez les définitions et les traductions éventuelles de : cookie, *phishing*, *malware*, *spyware*, *ransomware*, virus, ver, porte dérobée (*backdoor*), cheval de Troie, *keylogger*. (cf fiche de cours, Wikipedia, ANSSI)
5. +Trouver la charte informatique de l'université Paris-Saclay que vous avez signée en début d'année et la relire, en particulier le paragraphe concernant vos identifiants.

Exercice 1 +Authentification / Mot de passe

Objectifs : être attentif au risque d'atteinte à la confidentialité de ses données et à sa vie privée sur des services en ligne professionnels ou personnels (webmail, sites de partage de documents, de photos, réseaux sociaux etc.). Savoir protéger ses comptes à l'aide de choix et de procédures robustes concernant les identifiants et les mots de passe.

Question préalable : qu'appelle-t-on identification ? Authentification ?

1. Expliquer pourquoi, quel que soit le service numérique, nous n'avons pas le droit d'utiliser l'identifiant et le mot de passe d'un autre utilisateur à son insu.
2. L'administrateur système du service informatique du laboratoire où je fais mon stage me demande mon mot de passe au téléphone, pour faire des travaux de maintenance. Quelle est la meilleure attitude à adopter ?
3. +Donner des exemples d'erreurs classiques dans le choix d'un mot de passe.
4. +Proposer une procédure pour choisir un bon mot de passe.
5. +Quel type de mot de passe faut-il alors adopter ?
6. Quelles bonnes pratiques peut-on recommander concernant les identifiants et mots de passe ?

Exercice 2 Les cookies : les connaître et les gérer.

Objectifs : être attentif au risque d'exploitation d'informations personnelles lorsque l'on navigue sur le WEB. Connaître la notion de cookies, savoir où ils sont stockés, savoir comment les effacer.

Question préalable : qu'est-ce qu'un cookie ? Quels sont les différents types de cookies ? Lesquels nous sont utiles, lesquels nous espionnent ?

Effacer sélectivement et successivement les traces de votre navigation : historique, cache, cookies (cookies : distinguer la procédure d'effacement global de tous les cookies et l'effacement sélectif de certains cookies).

<u>Sur Firefox:</u>
Historique : menu Historique > Supprimer l'historique récent ; afficher les détails si l'on souhaite supprimer sélectivement certaines traces seulement ; choisir le jour à supprimer.
Attention ici ne pas cocher la cas cookies, sinon tous les cookies seront supprimés d'un coup.
Cookies : pour supprimer certains cookies seulement et pas tous, il faut aller dans Préférences > vie privée et sécurité > gérer les données > choisir lesquels, valider ensuite.
<u>Sur Chrome :</u>
Cliquer sur "Effacer les données de navigation". Il faut un peu chercher pour trouver où effacer sélectivement certains cookies et pas d'autres…

Exercice 3 Sécurité des transferts de données et des communications (web, mail, chat…)

Objectifs : savoir comment protéger ses données confidentielles (notion de données personnelles sensibles) et ses communications.

1. Les données bancaires sont des données personnelles sensibles. Que doit utiliser le serveur web de ma banque si je veux consulter des informations concernant mon compte de façon sécurisée ? Comment puis-je vérifier que c'est le cas ?

2. Si je souhaite que mes communications professionnelles ou personnelles (mail, chat…) ne soient pas espionnées, quel type de protection est nécessaire ? Le mail permet-il une telle protection ?

Exercice 4 Sécurité de ses équipements informatiques (virus, ver…) et de ses comptes (phishing…)

Objectifs : savoir sécuriser ses équipements informatiques (ordinateur ici) à l'aide de logiciels de protection et de comportements de prudence.

En général, les logiciels antivirus des grandes marques sont tous capables de reconnaître l'ensemble des virus connus.

1. Antivirus : pour quelle raison une machine équipée d'un tel produit peut tout de même se faire infecter ?
2. Antivirus : S'ils reconnaissent tous les mêmes virus, quel peut être l'avantage d'utiliser des produits de différentes marques ?
3. Risques du mail : pièces jointes.
   Vous recevez un courriel avec des fichiers joints, ceux-ci ont les extensions suivantes : exe, com , vbs, scr, doc, xls. Que faites-vous ?
   Même si l'expéditeur semble connu, une analyse de la pièce jointe à l'aide du « scanner » anti-virus avant de l'ouvrir n'est pas une mauvaise idée si vous possédez un anti-virus.
4. Risques du mail : phishing
   Lors de la réception d'un e-mail contenant un fichier en pièce jointe ou un lien vers un site web, il est utile de se poser quelques questions : est-ce que je connais l'expéditeur ?
   Si le mail est alarmiste (sur son compte mail qui va être coupé, son compte bancaire piraté..), que faites-vous ?
   Que faut-il examiner dans l'adresse mail elle-même ?
   Le contenu du mail lui-même (langue utilisée, signature, etc.) me permet-il d'être sûr que c'est bien lui qui a rédigé ce courrier ?

   Exemples de mails reçus, à commenter (au moins 1) :

TS **Thunersee Schiffcatering** 14 septembre 2018 à 01:04
Service Informatique Université Paris-Sud (UPSUD)

En ce moment, nous avons remarqué une tentative de connexion avec le mot de passe de votre compte à partir d'un lien de périphérique inconnu et une connexion pour valider et sécuriser votre boîte aux lettres dans les 24 heures. Sinon, vous risquez de perdre votre boîte aux lettres.

Cliquez ici pour l'authentification UPSUD

Équipe webmail

DF **DE MORONI Frederique** 14 août 2018 à 13:39
RE:Maintenance et opérations.
À : DE MORONI Frederique

De : DE MORONI Frederique
Envoyé : mardi 14 août 2018 11:58
Objet : Maintenance et opérations.

Votre compte Web Microsoft Outlook a récemment fait l'objet de modifications de sécurité au 6/1/2018. L'action requise est la suivante: Cet e-mail automatisé contient un lien permettant de réinitialiser et de gérer votre mot de passe Outlook Web App lorsque votre mot de passe actuel a expiré.

Cliquez ici pour accéder à la page Réinitialiser le mot de passe. Suivez les instructions ci-dessous pour créer un nouveau mot de passe.

Le nouveau mot de passe doit répondre aux critères du mot de passe:
*au moins 8 caractères.
* contenir au moins une lettre majuscule
* contenir au moins une petite lettre
* contient au moins un caractère spécial
* n'utilisez pas les 3 derniers mots de passe utilisés auparavant.
* n'incluez pas les 2 premiers caractères de votre nom d'utilisateur
exemple de bon mot de passe: A @ qr * 981

Le lien ci-dessus expire après 24 heures. Si vous ne modifiez pas votre mot de passe avant, votre compte Outlook Web App est verrouillé pour des raisons de sécurité.

Je vous remercie,
Maintenance et opérations.

Source: Équipe de sécurité du courrier électronique.

>>>>>> VEUILLEZ NE PAS RÉPONDRE À CE MESSAGE <<<<<<
Cette boîte aux lettres est utilisée pour les messages sortants SEULEMENT et n'est pas surveillée f10353

ZA **ZIMBRA ADMIN** 22 juillet 2019 à 10:30
Bonjour

Votre compte Zimbra a atteint 1.99 sur 2 Go que nous vous avons alloué (votre administrateur), ce qui signifie que vous avez utilisé jusqu'à 99% de vos Mo. Vous devez mettre à niveau votre compte maintenant pour continuer à recevoir et à envoyer des messages.

Cliquez ici pour mettre à jour votre compte: http://sdgfbvcv.tripod.com

Expéditeur
Zimbra Admin

5. + Dans quelle mesure les vers sont-ils plus dangereux que les virus ?
6. + Certains vers qui se propagent sur Internet ne provoquent aucun dommage sur les machines atteintes. Pourquoi sont-ils cependant nuisibles ?
7. + On considère dans cet exercice une variante du ver W32/Beagle. Ce ver se présente sous la forme d'un courrier électronique possédant un fichier joint qui est à la fois compressé et chiffré. Le mot de passe pour déchiffrer le fichier est contenu dans le corps du message. Si la victime exécute le fichier obtenu après décompression avec le mot de passe fourni (qui est un fichier avec une extension .exe), alors le ver se propage en choisissant la prochaine victime dans le carnet d'adresses de la victime courante.
   Pourquoi le fichier compressé est-il chiffré puisque le mot de passe est fourni dans le message ?
8. + Pour désinfecter un ordinateur, il est recommandé de le redémarrer depuis un CD-ROM ou une clef USB ; pourquoi ?
9. + Votre ordinateur en réseau est contaminé, que faites-vous ?

Exercice 5 + Porte dérobée et cheval de Troie

1. Comment un attaquant peut-il procéder pour installer une porte dérobée (*backdoor*) ?
2. Comment un attaquant peut-il procéder pour installer un cheval de Troie ?
3. Comment se protéger de ces deux malware ?

Exercice 6 Qualifier la nature d'un risque informatique (D, I, C, T) et le traiter

Objectif : savoir qualifier la nature d'un risque informatique (D, I, C, T) et savoir s'en protéger si le risque est important.

Question préalable : que signifient les 4 lettres qualifiant les risques informatiques D,I,C,T ? (cf fiche de cours).

Étude de cas : utilisation d'un ordinateur portable par un étudiant en thèse (doctorant) lors de ses déplacements dans un labo à l'étranger ou pour un colloque à l'étranger

- Le disque dur contient ses résultats de recherche, des informations stratégiques (articles de recherche sur son sujet de thèse, courriels échangés avec des partenaires industriels, brevet en voie de dépôt en cas de thèse CIFRE…) et des données privées de l'étudiant.
- Cet étudiant est amené à se déplacer régulièrement à l'étranger pour ses travaux de recherche (laboratoires pour collaborer, colloques…) et utilise son ordinateur dans des endroits publics exposés : aéroports, gares, hôtels...
- La seule protection utilisée est un simple couple identifiant/mot de passe à l'allumage de l'ordinateur.

Pour le cas de cet étudiant :

1. Définissez le type du risque (D, I, C, T).
2. Comment le traiter, le cas échéant ?
3. Quelles sont les conséquences pour l'étudiant s'il ne traite pas ces risques et que l'un se réalise ?

Exercice 7 Sauvegarde et archivage

Objectif : savoir comment sécuriser ses données professionnelles ou personnelles par des procédures de sauvegarde rigoureuses (en particulier, ses documents, collectés sur le web ou produits par soi-même - ses cours, ses propres rapports et mémoires etc.- ou ses documents personnels administratifs, photos etc.)

Complément de cours :

* Une bonne politique de sauvegarde consiste à :

- Faire plusieurs sauvegardes, car une des copies peut être défectueuse

- Sauver les données de façon régulière car lorsque des données sont détruites, vous perdez toutes les modifications depuis votre dernière sauvegarde. Si vous sauvegardez vos données toutes les semaines, vous perdrez au maximum 1 semaine de travail.

- Les sauvegardes ne doivent pas être toutes entreposées dans le même lieu. Si un incendie ravage votre appartement, ou si vous êtes cambriolé vous risquez de tout perdre. La technique la plus sure consiste à placer une de vos sauvegarde sur 1 serveur en ligne.

* Le **mirroring** : a pour but de dupliquer l'information à stocker sur plusieurs disques simultanément. Ce procédé est basé sur la technologie RAID (acronyme de Redundant Array of Inexpensive Disks, traduire ensemble redondant de disques indépendants) qui permet de constituer une unité de stockage à partir de plusieurs disques durs.

*** Backup** : Les logiciels de " backup " proposent de sauvegarder un ensemble de fichiers et de répertoires dans un fichier appelé archive. Ils offrent en général un grand nombre de fonctionnalités :

- Archivage et récupération des données.

- Compression des données.

- Planification des sauvegardes.

- Choix des différents répertoires et fichiers à sauvegarder.

- Choix de l'emplacement de l'archive : disque amovible, disque réseau,...

La bonne stratégie de sauvegarde

Compte tenu des multiples risques pesant sur vos données (panne, vol de votre machine, piratage informatique, etc.), il est indispensable de faire régulièrement des sauvegardes de vos données les plus précieuses vers (par exemple) un disque dur externe. Ceci implique de :

— Hiérarchiser vos données : Vos albums photos personnels sont uniques ! En revanche votre filmothèque peut être reconstituée en rachetant les films. Plus le volume de donnée est important, moins il est facile de faire des sauvegardes.

— Synchroniser vos données à sauvegarder plutôt que de réaliser des copies : vous gagnez du temps car les données qui n'ont pas changé ne sont pas copiées.

— Conserver les données à 2 endroits différents (pour éviter la perte de donnée lors d'incendie ou de cambriolage)

1) Quelles sont les deux méthodes de sauvegarde de données les plus fiables (en termes de localisation du support) ?

2) Quelle est la différence entre sauvegarde et archivage ?
cf article Wikipedia : https://fr.wikipedia.org/wiki/Sauvegarde_(informatique)

3) + Que signifie sauvegarde *totale ? différentielle* ? *incrémentale* ?

Exercice 8 Conditions d'utilisation des services en ligne[1]

Objectif : comprendre les divers modèles économiques des entreprises sur Internet et en particulier ceux des GAFAM. Connaître les conditions d'utilisation des services en ligne pour opérer des choix éclairés en amont d'une inscription éventuelle.

Question préalable : beaucoup de services en ligne (réseaux sociaux, sites de partage de photos ou de vidéos) sont gratuits pour l'utilisateur, que ce soit pour lire ou pour poster en ayant un compte. Comment ces entreprises (souvent l'une des GAFAM) génèrent-elles du profit ?

1. Services de partage de photos

Trouver l'URL des conditions d'utilisation d'Instagram. Quels droits cédez-vous relativement à vos contenus, par exemple les photos que vous publiez ?

Un site plus ancien mais fréquenté par des communautés de photographe est Flickr. L'entreprise qui possède Flickr a prévu de laisser les photographes choisir quel régime de droits ils souhaitent attacher à leurs photos, par exemple une des licences Creative Commons.

+ Rappeler ce que signifie « licence Creative Commons » et quelles sont ces licences (quels droit accordent-elles à l'utilisateur, par avance ?)

Conclure sur le respect des droits des utilisateurs par Instagram et Flickr.

2. + Services de partage de vidéos

Même questions concernant Youtube relativement aux vidéos postées par les internautes.

Comparer avec Vimeo, un autre site de partage de vidéos.

Conclure.

1 *Terms of service* (TOS) en anglais