01/09/22 : Dépôt des sujets de projets
Janvier 2023 ? : soutenance
Rapport à rendre une semaine avant la soutenance (incluant bibliographie)

Deux types de sujet :

- R&D
- Veille technologique

Projet R&D (apprentissage) équivaut plus ou moins au PIDR (statut étudiant)

80h minimum

Consignes pour le rapport : disponibles sur le livret d'apprentissage

1. Veille technologique

Définition Wikipédia
Où chercher l'information ?

- Internet (google, google scholar,...)
- Bibliothèques (livres, revues scientifiques,...)

2. R&D

Où chercher l'information ?

- Internet (google, flux RSS,...)
- Bibliothèques (revues scientifiques,...)

Pour la bibliographie : ~~faire un excel en recensant tous les livres/articles intéressants + faire légende sur ce qui a déjà été lu/étudié~~
utiliser **Save to Notion**

Lecture en 2 temps :

- Rapide : résumé, introduction, conclusion
- Approfondie : article complet (induisant d'autres recherches, analyse des résultats)

- **Blindez vos data avec... un téléphone crypté**

  Oué

- **Blindez vos data avec... un clavier virtuel**

  Clavier d'ordinateurs ⇒ passoire d'informations (keyloggers ou enregistreur de touches)
  Keylogger ⇒ logiciel installé caché qui permet de recenser toutes les touches // petit câble entre le clavier et l'ordinateur
  Banques sont les premières à adopter ce procédé
  Interception du signal d'un clavier sans fil ⇒ vente de clavier sans fil cryptés par Microsoft (ou filaire tout simplement …)

- **Blindez vos data avec… un coffre-fort électronique**

  Description:
  Cette solution s'adresse aux entreprises, soucieuses de la sécurité de leurs documents qui les engagent auprès de tiers (factures, contrats, fiches de paie..). Contrairement à un coffre fort physique, l'entassement de papier et la désorganisation n'est pas d'actualité, ici il s'agit plus de récupérer de façon efficiente les documents stockés (moteur de recherche) mais également d'en garantir leur sécurité lorsqu'il s'agit d'y accéder (limitation d'accès). Toutes les opérations de consultation et modifications sont tracées (horodatage).

  Conseils de sécurité:
  L'entreprise doit être la seule à pouvoir accéder aux données et les informations stockées doivent être cryptées à chacune des étapes du processus (entrée/sortie) par une clé qui remplit les exigences de l'Agence nationale de la sécurité des systèmes d'information. Il est préférable que ce coffre virtuel soit hébergé en France ou dans tout autre pays qui ne pourra pas légalement accéder aux données stockées (contrairement aux Etats Unis avec la loi Acta)

- **Blindez vos data avec... Confide, le Snapchat pour professionnels**

  Reprise du concept des images éphémères (c'est le seul point commun avec Snapchat)
  Envoie de messages txt uniquement (mail, sms) qui seront automatiquement détruit une fois envoyé et lu
  Sécurité renforcée, impossible de prendre une capture d'écran, transport des msg chiffrés…
  alerte si tentative de capture d'écran, message lisible mot par mot
  Question de l'utilisation illégale ? comme télégram par ex
  service pour pc maybe ?

- **Blindez vos data avec… une borne de décontamination USB**

Cet article traite dans un premier temps des dangers des clés USB contaminées qui peuvent contenir de potentiels virus et infecter les ordinateurs du serveur d'une entreprise (des chiffres sont donnés). Un moyen de contrer cela est la mise en place de bornes de décontamination USB dans les entreprises (exemple de USB malware cleaner de Lexsi). Elles auront pour but d'analyser les virus potentiels présents dessus et de les mettre en quarantaine et éviter toutes fuites de données ou pollution de leurs espaces de travail numérique. La clé pourra derrière être utilisée en toute sécurité derrière. Une autre possibilité donnée par l'article est le fait de fournir des clés USB "vaccinées" contre les virus les plus courants aux employés.

En effet, les chiffres donnés par l'article sont les suivants :

- 1/4 des infections sur les Système d'Exploitation le sont par clé USB (26%)
- 66% des employés sont prêts à brancher une clé USB qu'ils trouvent sur leur ordinateur pro => pas de sensibilisation

- **Blindez vos data avec... un logiciel de protection des applications mobiles**

  De + en + de gens ont une tablette / téléphone intelligent => C'est dangereux et tout à travers le téléchargement d'application ou même les hotspots gratuit, donc on est de + en + confronté à des logiciels malveillants. Thalès, Symantec ou encore Denyall ont créé des programmes qui protègent les environnements mobiles. Système d'authentification pour séparer les données perso / pro, ainsi que des systèmes de cryptage de données et de communication. Mise en place de magasins d'applis sécurisées…

- **Blindez vos data avec… des tests de pénétration**

  Attaques des systèmes d'information par des hackers blancs (souvent entreprise de service) pour en connaître les vulnérabilités et donc les corriger ainsi que de tester la réactivité des clients
  Utilisation des techniques de pénétration connues (cheval de troie, DoS, …)
  Tests en interne ou externe, en temps limité et régulièrement pour rester pertinent face aux nouvelles menaces.