

<u>DESIGN, INNOVATION ET CRÉATIVITÉ</u>	4 ^{ème}
<i>Je veux ma clef !</i>	

- x Bernard, retraité, passionné de photos animalière (ornithologie) qui veut se lancer dans le traitement informatique de l'image.
- x Jimmy, guitariste/musicien, leader d'un groupe, sauvegarde ses compositions sur ordinateur, et veut les proposer à des producteurs.
- x Paula, arbitre de basket, doit enregistrer les résultats des matches pour les envoyer à la fédération (FFB).
- x John, professeur d'anglais pour les entreprises, tous ses documents (cours, présentation...) sont stockés sur sa clef USB qu'il connecte aux ordinateurs des entreprises dans lesquelles il intervient.
- x Thierry, technicien sur les réseaux informatiques,

Ces personnes ont comme point commun la volonté de ne pas vouloir utiliser de « cloud » pour stocker leurs fichiers (photos, documents...).

Ils utilisent une ou plusieurs clefs USB, sachant que celles-ci ont une capacité de stockage de plus en plus importante (64, 128... Go).

Travail demandé :

A partir de la cible (il faut choisir une de ces personnes), imaginez en détail à l'aide de mots, les conditions dans lesquelles se trouve/est utilisée la clé USB.

Pour débiter cette analyse, sur une feuille (de classeur), dresser la liste des situations/endroits/espaces, où la clef peut se retrouver, et la liste des goûts des utilisateurs, cela en fonction de leurs « profils ».

<u>DESIGN, INNOVATION ET CRÉATIVITÉ</u>	4^{ème}
<i>Je veux ma clef !</i>	

LE CLOUD, LES DATA CENTERS ET L'ÉNERGIE

- Source : UFE (23 janv. 2017)

Le développement constant des usages numériques a entraîné une multiplication par 4,5 du trafic mondial de données (« data ») entre 2011 et 2016 selon l'ARCEP⁽¹⁾. Ces flux d'informations liés aux échanges dématérialisés entraînent une consommation d'énergie bien réelle (matériel informatique, succession de routeurs pour la transmission d'informations, data centers pour le traitement et le stockage de données, etc.). En France, la consommation électrique des data centers aurait atteint près de 3 TWh en 2015 selon RTE, soit davantage que la consommation électrique annuelle de la ville de Lyon.

Dans cette courte note de l'Observatoire de l'électricité publiée le 18 janvier, l'Union française de l'électricité (UFE)⁽²⁾ rappelle le principe du « cloud computing » qui s'oppose au stockage et à la gestion locale de l'information. Encore abstrait pour de nombreux utilisateurs, ce « cloud » se matérialise par des data centers « externalisés »⁽³⁾ de plusieurs centaines ou milliers de mètres carrés dans lesquels des rangées de serveurs stockent, gèrent et rendent disponibles des informations via Internet.

L'UFE comptabilise en France plus de 180 data centers de ce type qui sont pour un tiers d'entre eux situés en Ile-de-France. La facture énergétique de ces sites (électricité pour le traitement des données mais aussi pour la climatisation) constitue en moyenne 40% de leurs coûts de fonctionnement. Le prix et la « qualité » de l'électricité font ainsi partie des enjeux majeurs de ce secteur.

La France présente à ces égards des conditions favorables pour installer des data centers (avec des prix de l'électricité en moyenne inférieurs par rapport aux voisins européens), souligne l'UFE qui insiste sur les retombées économiques locales associées à l'implantation de ces sites (en matière d'emploi et pour développer « un écosystème favorable à la digitalisation d'un territoire »). Différents acteurs développent par ailleurs de nouveaux modèles pour réduire cette lourde facture énergétique et valoriser notamment la chaleur émise par les équipements électroniques de leurs data centers.

En amont de ce traitement de données, l'Ademe rappelle fréquemment la responsabilité des internautes (ici peu abordée) dans la consommation électrique croissante des data centers qui pourrait être réduite par des actions simples : limiter le nombre de destinataires des courriels, effectuer un tri régulier dans sa boîte mail, etc⁽⁴⁾. A titre indicatif, l'envoi d'un mail avec pièce jointe de 1 Mo transitant sur différents serveurs entraîne à lui seul une consommation électrique aussi importante qu'une ampoule basse consommation de 20 watts allumée pendant une heure. Au niveau mondial, près de 215 milliards de mails (hors spam) auraient été envoyés en 2016 selon Radicati Group.

<u>DESIGN, INNOVATION ET CRÉATIVITÉ</u>	4^{ème}
<i>Je veux ma clef !</i>	

Sources / Notes :

1. Autorité de régulation des communications électroniques et des postes
2. Site de l'UFE
3. Non intégrés dans des entreprises.
4. « Internet, courriels : réduire les impacts », Ademe, février 2014.

QUELS SONT LES RISQUES DE SÉCURITÉ MAJEURS DU CLOUD (COMPUTING) ?

Une étude du CSA en révèle douze

Ce sont notamment :

1. L'existence de brèches de sécurité tant sur l'une des couches logiques du Datacenter que celles issues d'erreurs humaines ;
2. La fragilité dans la gestion des accès et des identités, bien que certains fournisseurs renforcent les interfaces d'authentification avec d'autres moyens tels que les certificats, les smartcards, la technologie OTP et bien d'autres ;
3. L'utilisation d'API non sécurisées pour l'intégration des applications avec les services cloud ;
4. L'exploit de vulnérabilités des systèmes d'exploitation sur les serveurs du cloud et même sur les applications hébergées ;
5. **Le piratage de compte**, qui est un vieux type d'attaque informatique, vient avec une forte recrudescence depuis l'avènement d'Internet et encore celui du cloud computing ;
6. **Une action malveillante initiée en interne dans les effectifs du fournisseur**. Une personne malveillante dans l'équipe de gestion du Datacenter peut facilement nuire à la confidentialité et l'intégrité des environnements hébergés ;
7. **Les menaces persistantes avancées** (en anglais, APT : Advanced Persistent Threats) qui consistent en une forme d'attaque où le hacker réussit à installer d'une façon ou d'une autre un dispositif dans le réseau interne de l'organisation, à partir duquel il peut extirper des données importantes ou confidentielles. C'est une forme d'attaque difficile à détecter pour un fournisseur de services cloud ;
8. **La perte de données** qui peut être causée par une attaque informatique (logique) du Datacenter, une attaque physique (incendie ou bombardement), une catastrophe naturelle, ou même simplement à un facteur humain chez le fournisseur de services, par exemple en cas de faillite de la société ;
9. Les insuffisances dans les stratégies internes d'adoption ou de passage au cloud. Les entreprises ou les organisations ne prennent pas souvent en compte tous les facteurs de sécurité liés à leur fonctionnement avant de souscrire à un service cloud. Certaines négligences, tant au niveau du développement d'application qu'au

<u>DESIGN, INNOVATION ET CRÉATIVITÉ</u>	4 ^{ème}
<i>Je veux ma clef !</i>	

- niveau de l'utilisation basique, leur sont parfois fatales ;
10. Utilisation frauduleuse des technologies cloud en vue de cacher l'identité et de perpétrer des attaques à grande échelle. Généralement, il s'agit de comptes créés pendant les périodes d'évaluation (la plupart des FAI proposent 30 jours d'essai gratuits) ou des accès achetés frauduleusement ;
 11. Le déni de service qui est une attaque qui consiste à rendre indisponible un service par une consommation abusive des ressources telles que les processeurs, la mémoire ou le réseau. L'idée, pour le pirate, c'est de réussir à surcharger les ressources du Datacenter en vue d'empêcher d'autres utilisateurs de profiter des services ;
 12. Les failles liées à l'hétérogénéité des technologies imbriquées dans l'architecture interne du cloud, et l'architecture externe d'interfaçage avec les utilisateurs.