Présentation Ardiac – 14 déc 2017

Sécurité informatique : sensibilisation & bonnes pratiques

Qui sommes nous

MCC INFORMATIQUE

Informatique & Téléphonie

Installation & Maintenance

Jean-Pierre UCHAN

Patrice BRIDOUX

Sauvegarde

- La seule vraie et unique protection
  - Avoir plusieurs copies !
- Quotidienne (ou plus si besoin)
- Prévoir un archivage
- Dans un autre bâtiment
  - Attention aux conditions d'utilisation du cloud !
- Restauration pour vérifier de temps en temps

Mots de passe

- Ne pas utiliser un mot de passe plusieurs fois
  - tous vos accès seraient compromis en une seule fois
- Ne pas utiliser de mot de passe trop simple
  - dans le top 10 des mots de passe : 123456, qwerty, 123456789, 111111, password, 123123
  - pas de mots du dictionnaire
  - ni votre prénom, votre nom

Mots de passe

- Au moins 1 majuscule
- Au moins 1 minuscule
- Au moins 1 chiffre
- Au moins 1 caractère spécial
- 8 caractères minimum
- Ne doit rien signifier
- Ae2laP:€ par exemple (avec astuce !)

Mots de passe

- Utilisé tous les jours, il se retient facilement
- On peut utiliser une phrase ou les premières lettres des mots d'une phrase
- On peut utiliser un gestionnaire de mot de passe avec un mot de passe principal (Firefox ou KeePass)
- Préférer Chromium à « Google Chrome »
- Ne pas laisser les mots de passe par défaut
  - Dans vos ordinateurs
  - Dans vos équipements actifs (box, switch)

Mises à jour

- Tous les systèmes contiennent des bugs
- Qui créent des failles de sécurité
- Que des logiciels malveillants peuvent exploiter
- Pour détourner vos ressources informatiques
- Dans certains cas vos données
- À votre préjudice ou au préjudice d’autres
- Souvent, sans que vous ne puissiez rien voir

Mises à jour

- Les mises à jour des systèmes et des programmes
- Doivent être réalisées avec assiduité
- De manière automatique dès possible
- Malgré les risques de régressions
- Ne pas télécharger et installer des logiciels dont la provenance est incertaine

Séparation des privilèges

- Utilisez un compte sans privilèges pour
  - les besoins quotidiens / standards
- N’utilisez le compte administrateur que pour
  - l’installation de logiciels
  - la configuration de la machine
  - les mises à jour

Matériels

- Attention à l’accès à votre matériel
  - Accès physique = pas de sécurité
  - Ne pas perdre de vue vos équipements informatiques
- Attention aux connexions avec des équipements inconnus
  - Smartphone
  - Clé usb (gros vecteur d’attaque !)
  - Point de charge public

Smartphone

- C’est d’abord un ordinateur avec une connexion réseau
  - Donc très intéressant pour les pirates
  - Pas bien (ou pas du tout) mis à jour
- Un véritable espion dans votre poche
  - Qui suit tous vos mouvements
  - Écoute votre environnement (éventuellement en permance)
  - Livre vos données à des tiers

Wifi (chez vous)

- Une prise vers votre réseau, sur le trottoir
  - Ne pas le laisser actif si vous ne l’utilisez pas
- Sécurisez l’accès
  - Clé WPA2 seulement, pas de WEP, ni WPA
  - Un mot de passe sérieux

Wifi et point d’accès public

- Attention au wifi public
  - Rien ne garanti que votre trafic n’est pas écouté
  - Utilisez un vpn (tunnel crypté entre vous et l’Internet)
  - Utilisez des protocoles sécurisés (https, imaps, ...)
- Attention aux équipements qui ne sont pas à vous
  - Peut être enregistrent-ils tout ce que vous faites ?
  - (Inclus les mots de passe que vous utilisez !)

Disques / données mobiles

- Parce qu'il est facile de les perdre
  - Ou de se les faire voler
- Protéger par mot de passe
  - Les fichiers sensibles
- Crypter tout le disque
  - Ce qui protège tout le système et son contenu

Mail

- Ne pas faire confiance au champ De: (l'expéditeur)
  - N'importe qui peut y mettre n'importe quoi
  - Les systèmes antispam aide (un peu)
- Attention avec qui vous parlez
  - Ne jamais répondre aux chaînes, appels à solidarité, alertes de sécurité, alertes virales, etc.
  - Les mails vers quelquun@gmail.com sont lus, analysés et stockés pour toujours chez Google (donc pas vraiment privé)

Mail

- Pensez à vos correspondants !
    - Attention aux envois groupés
        - Ne pas utiliser le champ Cc:
          ce qui expose vos contacts (votre richesse)
        - Utiliser le champ Cci:
        - Ou mieux, utilisez des services professionnels
          de type Mailjet ou Sendinblue ou Mailchimp

Mail

- Ne pas faire confiance aux liens Internet
  - Survolez le lien (qui apparaît alors en bas à gauche)
  - https://machin.truc.chose.fr/ici/la/ailleurs.html?x=y&z=nnnnnnnn
  - Ne cliquez dessus que si la destination vous convient
  - Redoublez d'attention si le lien vous demande un mot de passe
- Ne pas faire confiance aux fichiers attachés
  - Attention d'avoir un antivirus bien à jour
  - N'ouvrez (et surtout pas en automatique) que si vous êtes sûr

Web

- Attention, vous lisez le web mais le web vous observe aussi !
- Google, Facebook, Twitter et d'autres enregistrent votre trafic que vous soyez connectés chez eux ou pas
- Google a admis avoir des fiches nominatives sur tous les humains de la planète
- Il convient de considérer qu'il n'y a pas de vie privé en ligne (à moins d'utiliser tor)

E-commerce

- Essayez d’évaluer la réputation du site e-commerce
  - Amazon, Les 3Suisses sont à priori fiables
- Vérifiez que vous êtes bien en https:// (cadenas vert)
  - Et donc le trafic entre vous et votre correspondant est crypté
- Vérifiez l’adresse du site de paiement
  - Par exemple https://xxxx.leprestataire.com/zzzzzz
  - Vous allez accorder votre confiance à « leprestataire.com »
  - A vous d’apprécier...

Conclusion :
Sécurité contre Liberté

- Un curseur à régler pour adapter le niveau de sécurité aux usages et contraintes de chacun.

Pour aller plus loin

- Agence nationale de la sécurité des systèmes d'information
  https://www.ssi.gouv.fr
- Et son Guide des bonnes pratiques de l'informatique
  https://www.ssi.gouv.fr/uploads/2017/01/guide_cpme_bonnes_pratiques.pdf
- CNIL – Informatique et libertés
  https://www.cnil.fr/
- Mais aussi
  - Cryptage des disques :
    - Windows 10 : https://docs.microsoft.com/fr-fr/windows/device-security/bitlocker/bitlocker-overview
    - Linux : https://doc.ubuntu-fr.org/tutoriel/chiffrer_son_disque
    - MAC OS X : https://support.apple.com/fr-fr/HT204837

- Wikipédia https://fr.wikipedia.org/wiki/Sécurité_des_systèmes_d'information
- Centre gouvernemental de veille (pour les plus motivés;) https://www.cert.ssi.gouv.fr/