LES REGLES ELEMENTAIRES DE SECURITE

LE POSTE DE TRAVAIL

CNRS – RSSIC – version du 11 mai 2012

Un poste de travail mal protégé peut mettre en péril non seulement les informations qui sont traitées sur le poste lui-même, mais également les systèmes auxquels il se connecte. Une fois piraté, il peut devenir une porte d'entrée vers des systèmes plus sensibles dès lors qu'un logiciel espion a pu être installé à l'insu de l'utilisateur. **L'équipe chargée du support informatique* est mandatée par le Directeur d'unité pour faire appliquer les mesures techniques afférentes aux règlements de sécurité.**

Le comportement de l'utilisateur de ce poste de travail est essentiel, s'il applique les règles élémentaires de sécurité, il va renforcer la sécurité de ce poste et de l'ensemble des systèmes auxquels il se connecte ou bien, au contraire, s'il n'observe pas ces règles, il va faciliter le travail des pirates et mettre à mal les efforts de l'ensemble de la communauté de travail.

Le Directeur d'unité est responsable de la sécurité des systèmes d'information de son unité, il a la responsabilité de faire connaitre et de faire appliquer les règlements de sécurité (politiques de sécurité, chartes, règles) promulgués par les tutelles dont il dépend.

Il est essentiel que les *règles élémentaires de sécurité* soient connues et mises en œuvre par l'équipe informatique et les utilisateurs, elles reposent sur :

- **La protection technique du poste de travail**
  - **Sauvegarde systématique et quotidienne des données**
  - **Configuration maîtrisée et mise à jour régulièrement**
  - **Chiffrement des supports de stockage (postes nomades, clés, disques, etc.)**
- **Un comportement avisé de l'utilisateur**
  - **Protection de son poste de travail contre le vol et les accès illégitimes**
  - **Mots de passe robustes et personnels**
  - **Attitude prudente vis-à-vis des supports de données amovibles (clés USB, etc.)**
  - **Utilisation prudente d'Internet (téléchargements, utilisation de services en ligne)**
  - **Attitude prudente vis à vis des messages reçus**
  - **Alerte des responsables techniques et sécurité en cas d'évènement anormal**

Ces ***règles élémentaires de sécurité*** sont détaillées dans ce document.

*contacter votre informaticien ou celui de la DR / de l'université

LA PROTECTION TECHNIQUE DU POSTE DE TRAVAIL

1. **Sauvegarde systématique et quotidienne des données ***

   En cas de vol, de problème technique, ou d'attaque informatique sur le poste de travail, les données du poste de travail seront perdues s'il n'y a pas de sauvegarde.

   Souvent les utilisateurs regrettent amèrement de ne pas avoir pris leurs précautions avant qu'il ne soit trop tard.

   Les bonnes pratiques :

   - *Il convient donc d'organiser la sauvegarde des données pour les postes de travail fixes et portables, de la façon la plus simple possible pour l'utilisateur, afin que cette sauvegarde puisse être réalisée de la façon la plus régulière possible.*

2. **Configuration maîtrisée et mise à jour régulièrement ***

   Au quotidien des dizaines de failles sont découvertes dans les systèmes (Windows, MacOS, Linux, etc.) et logiciels (Acrobat Reader, Outlook, Word, etc.) qui équipent le poste de travail, ces failles sont très rapidement exploitées par des virus ou par des kits que mettent en ligne les pirates les plus expérimentés.

   Ces kits sont ensuite utilisés par la masse des pirates pour tenter de prendre la main sur le maximum de postes de travail et serveurs.

   Un compte ayant les droits « administrateur » permet de tout faire, sans aucun contrôle, sur tous les postes de travail en réseau, voire certains serveurs de l'unité.

   Les logiciels espions propagés par des sites alléchants, ou des pièces jointes de mails accrocheurs, « chassent » les comptes administrateurs pour ensuite « faire leur marché » dans vos données. Ces logiciels s'exécutant à partir d'une application lancée par un utilisateur n'ayant pas les droits d'administrateur feront, très souvent, beaucoup moins de dégâts et, la plupart du temps, seront totalement inefficaces.

   Les bonnes pratiques :

   - *Il est donc important de désactiver les programmes qui ne sont pas indispensables au bon fonctionnement du poste de travail, ils sont autant de portes que les pirates pourront utiliser pour tenter de pénétrer sur ce poste*

   - *Il convient d'utiliser au quotidien et en particulier pour naviguer sur internet un compte ne possédant pas les privilèges « administrateur »*

   - *De façon exceptionnelle certains utilisateurs doivent pouvoir obtenir un compte « administrateur » et le mot de passe associé, ces exceptions doivent être justifiées et validées par le directeur de l'unité. Dans ce cas, pour les opérations, comme des mises à jour, qui demandent les droits « administrateur » on utilisera préférentiellement les mécanismes du système d'exploitation qui permettent temporairement d'élever ses privilèges (sudo sous Unix et dérivés (LinuX, Mac, FreeBSD...), UAC ou « Exécuter en tant qu'administrateur » sous Windows).*

*contacter votre informaticien ou celui de la DR / de l'université

- *Il convient de désactiver l'exécution automatique des média amovibles*
- *Il convient d'installer un anti-virus sur le poste de travail*
- *Il indispensable de s'abonner à un service de mise à jour qui permette de garantir une mise à jour « au fil de l'eau » des principaux composants présents sur les postes de travail et des bases de signatures des virus découverts*
- *Il est utile de protéger le poste de travail par un pare feu qui filtrera les tentatives d'accès illicites depuis Internet*

3. Chiffrement des supports de stockage (postes nomades, clés, disques, etc.)

Les postes de travail sont de plus en plus légers et portables, leur exposition au vol a considérablement augmenté ces dernières années.

Or le poste de travail contient les données de travail mais également tous les codes d'accès aux réseaux, à la messagerie, aux applicatifs ainsi que les certificats électroniques permettant l'accès aux services en ligne et la signature de messages et de documents.

Les bonnes pratiques :

- *Il est indispensable de chiffrer les supports de stockage de données exposés au vol, en premier lieu les disques durs des PC portables.*
- *De même tout support amovible peut facilement être égaré ou volé, en particulier, il convient donc de chiffrer également les disques USB externes.*
- *Le chiffrement des disques internes et externes s'effectue en suivant les recommandations de la DSI du CNRS https://aresu.dsi.cnrs.fr/spip.php?rubrique99).*
- *Les clés USB ne doivent être utilisées que pour transférer les données et non pas comme un moyen de stockage (risque de perte de données important).*
- *Si la clé USB est utilisée pour transporter des sonnées sensibles, il est recommandé d'utiliser les clés USB auto-chiffrantes http://www.dsi.cnrs.fr/service/securite/Documents/corsair-padlock2.htm préconisées par la DSI du CNRS pour éviter le vol de données en cas de perte de la clé.*

*contacter votre informaticien ou celui de la DR / de l'université

UN COMPORTEMENT AVISE DE L'UTILISATEUR

1. Protection de son poste de travail contre le vol et les accès illégitimes

Les vols d'ordinateurs, de plus en plus fréquents, remettent en cause la confiance que nous portent nos partenaires industriels et dégradent l'image de marque des unités touchées. Ces vols réduisent à néant nos efforts de recherche : perte des données de recherche, vol d'informations par des équipes concurrentes, par des sociétés tierces, etc. In fine ces vols pourraient avoir des conséquences juridiques importantes pour notre organisation.

Les vols se produisent souvent par manque de vigilance, non seulement dans les transports en commun, en France et lors des déplacements à l'étranger, mais également dans les laboratoires, y compris très sensibles, par négligence, lorsque notamment les bureaux ne sont pas fermés à clé en cas d'absence.

Par ailleurs, le prêt de l'ordinateur à des tiers, famille, amis ou autres tierces personnes, peut donner un accès illégitime aux informations professionnelles qui sont soumises au secret professionnel et parfois à d'autres règlementations (secret industriel, etc.). Le comportement de ces tiers peut aboutir à l'installation volontaire ou involontaire de programmes malveillants sur cet ordinateur ou à l'utilisation volontaire ou non des logiciels professionnels avec détournement potentiel de leur usage.

Les bonnes pratiques contre le vol :

- *Au bureau*
  - *Fermer à clé la porte de son bureau*
  - *Attacher l'ordinateur portable avec un câble*
- *Dans les transports*
  - *Ne pas oublier son matériel … nombre de disparitions d'ordinateur résultent d'un simple oubli*
  - *Ne pas laisser son matériel en vue (dans une voiture, dans un train, etc.)*
  - *Ne pas laisser son matériel sans surveillance (en particulier dans les trains)*
  - *Mettre un signe distinctif sur l'appareil et sa housse pour le surveiller plus facilement et éviter les échanges volontaires ou involontaires (à l'aéroport par exemple)*
- *De plus lors de déplacements à l'étranger*
  - *Prendre en compte les conseils suivants : http://www.securite-informatique.gouv.fr/IMG/pdf/Passeport-de-conseils-aux-voyageurs_janvier-2010.pdf*

Les bonnes pratiques vis à vis du prêt à des tiers :

- *Le prêt ne peut être que très ponctuel dans e temps en cas de réelle nécessité (votre poste de travail n'est pas une console de jeux …)*
- *Rester près de la personne qui utilise votre ordinateur pour vérifier qu'il n'accède pas à des données professionnelles et qu'il ne cherche pas à modifier la configuration de votre ordinateur (installation de logiciels, etc.)*

*contacter votre informaticien ou celui de la DR / de l'université

2. Mots de passe robustes et personnels

Le mot de passe est la clé d'accès à l'information, cette clé doit être personnelle et suffisamment complexe pour ne pas pouvoir être trop facilement découverte – il existe des organisations qui louent de puissantes machines ou des réseaux de machines pour tenter de casser les mots de passe des utilisateurs qui détiennent des informations monnayables.

Les bonnes pratiques :

- *Un mot de passe doit rester personnel, pas de mot de passe partagé entre plusieurs utilisateurs*
- *Un mot de passe doit être suffisamment complexe (utilisation d'un mélange de lettres, chiffres et ponctuation, longueur minimum de 8 à 12 caractères en fonction du risque acceptable pour l'utilisateur et de l'effort qu'il est prêt à produire pour se protéger).*
- *Un mot de passe doit être changé assez régulièrement*
- *Un mot de passe doit être changé dès que l'on soupçonne sa compromission (vol ou perte du PC, divulgation à un tiers, etc.)*
- *Un mot de passe ne doit pas être accessible sans protection (par exemple affiché sur un post-it collé sur le tableau ou bien en vue sur le bureau …)*
- *Il est recommandé d'utiliser des mots de passe différents sur chacun des sites sur lesquels on se connecte. Comme cela est humainement très difficile, il est conseillé d'utiliser un outil de gestion des mots de passe tel que Keepass (http://www.projet-plume.org/fiche/keepass) qui permet de n'avoir qu'un seul mot de passe à retenir pour déverrouiller le coffre-fort contenant l'ensemble des mots de passe**
- *Il est recommandé de configurer son navigateur pour qu'il demande de choisir au cas par cas les mots de passe qu'il peut retenir lorsqu'il se connecte garder cette fonctionnalité (comme les forums divers, les sites commerciaux ne possédant pas vos coordonnées bancaires, etc. et, lorsque votre navigateur dispose de cette fonction, configurez le mot de passe maître qui permet de chiffrer les mots de passe enregistrés.**

NOTA : un ordinateur allumé avec une session utilisateur ouverte, laissé sans surveillance, même peu de temps (pause-café, etc.) permet à un intrus d'usurper facilement votre identité sans votre mot de passe principal et même de voler les autres mots de passe présents sur le poste de travail.

3. Attitude prudente vis-à-vis des supports de données amovibles (clés USB, etc.)

Les clés USB sont un vecteur de plus en plus utilisé pour le piratage des postes de travail.

Une clé peut s'infecter lors d'une utilisation sur un matériel infecté (une machine commune destinée aux présentations par exemple).

Une clé USB d'origine inconnue peut contenir des virus qui tenteront de s'installer sur le poste de travail, elle peut également être configurée pour « aspirer » le contenu du poste de travail à l'insu de son propriétaire.

De la même façon, la connexion de disques externes non maîtrisés expose au même danger dans la mesure où ces médias peuvent contenir un code malveillant susceptible de s'exécuter automatiquement, sans contrôle, sur le poste de travail.

*contacter votre informaticien ou celui de la DR / de l'université

Les bonnes pratiques :

- *Il est préférable d'apporter sa propre clé USB pour un échange de données, plutôt que d'utiliser une clé inconnue*
- *Il est utile de séparer les usages entre les supports utilisés à des fins personnelles (clés USB et/ou disques externes) et les supports utilisés à des fins professionnelles.*

4. Utilisation prudente d'Internet (téléchargements, utilisation de services en ligne)

Lorsque le poste professionnel est utilisé à des fins personnelles le périmètre de la navigation s'étend et l'on peut rapidement se retrouver sur un site malveillant.

Certains sites malveillants profitent des failles des navigateurs pour récupérer les données présentes sur le poste de travail. D'autres sites mettent à disposition des logiciels qui, sous une apparence anodine, peuvent prendre le contrôle de l'ordinateur et transmettre son contenu au pirate à l'insu de son propriétaire.

Il est très pratique d'utiliser les services disponibles sur Internet, parfois même ces services sont gratuits ce qui rend leur utilisation encore plus alléchante.

Il est important de bien comprendre que ces services ne donnent en fait aucune garantie sur l'utilisation qui sera faite des données stockées, parfois même certains sites indiquent – certes en petits caractères – que les données pourront être transmises à des tiers pour des raisons techniques ou légales et que l'on en cède quasiment tous les droits. Ainsi le *Patriot Act* permet aux services américains d'accéder aux informations stockées aux USA ou dont l'hébergeur est une société américaine. De même le contenu des informations est analysé afin de le revendre à des annonceurs pour de la publicité ciblée et peut-être à d'autres dans les cas extrêmes (l'intelligence économique).

Les bonnes pratiques :

- *Il est prudent d'éviter de se connecter à des sites suspects*
- *Il est prudent d'éviter de télécharger des logiciels dont l'innocuité n'est pas garantie (pérennité du logiciel, nature de l'éditeur, mode de téléchargement, etc.).*
- *Les sauvegardes de données, les partages d'information, les échanges collaboratifs, ne doivent se faire que sur des sites de confiance, mis à disposition par l'établissement et dont la sécurité a été vérifiée par l'établissement (via par exemple un audit de sécurité).*
- *Dans le cas où des données doivent impérativement être stockées sur des sites tiers ou transmises via des messageries non sécurisées, il conviendra alors de les chiffrer.**

*contacter votre informaticien ou celui de la DR / de l'université

5. Attitude prudente vis à vis des messages reçus

Nous sommes toujours tentés de savoir qui nous écrit, cependant de nombreux escrocs et pirates utilisent notre curiosité et notre crédulité pour tenter de voler nos données.

Dans certains cas le message frauduleux demande le changement du mot de passe d'un compte et redirige l'utilisateur vers un site pirate qui va voler ce mot de passe (c'est le « phishing ») *pour utiliser le compte de l'utilisateur à son insu et ainsi pénétrer dans sa messagerie, son compte bancaire, etc.*

Dans d'autres cas le message contient une pièce jointe piégée qui va installer un logiciel espion sur le poste de travail.

Les bonnes pratiques :

- *Il convient de supprimer les messages suspects, y compris s'ils proviennent d'une personne connue (son adresse a pu être « volée » sur une autre machine) si possible sans les ouvrir Lorsqu'un message suspect a été ouvert, il convient de ne pas répondre à l'expéditeur, , ne pas cliquer sur les liens présents dans le texte, ne pas ouvrir les pièces jointes*

- *NOTA : par ailleurs, les messages suspects identifiés comme indésirables par le système de messagerie seront automatiquement supprimés par le client de messagerie, il convient bien entendu de ne pas les ouvrir.*

6. Alerte des responsables techniques et sécurité en cas d'évènement anormal

Lorsqu'un évènement suspect se produit, il est indispensable d'alerter le support informatique, et le chargé de la SSI dans le laboratoire en cas d'incident de sécurité avéré.

Le chargé de la SSI (CSSI) prendra en compte l'incident et remontera l'alerte au niveau régional (RSSI de la DR) si la qualification de l'incident permet de suspecter un problème grave. Le RSSI de la DR remonte l'alerte au niveau national (équipe RSSI du CNRS) qui assure un suivi des incidents de sécurité et apporte un support au niveau régional en cas de besoin.

Il est important de noter :

- *qu'une attaque locale peut déboucher sur une atteinte nationale*
- *que le signalement d'un incident permet de s'assurer que les actions nécessaires sont bien entreprises*
- *que le suivi national des incidents permet de détecter des phénomènes invisibles au plan local*

*contacter votre informaticien ou celui de la DR / de l'université