N.Denos – K.Silini
BY-NC-SA

D1.2 :Sécuriser son espace de travail local et distant

N.Denos – K.Silini
BY-NC-SA

Les risques

Journée noire :
« Le disque dur de mon ordinateur est tombé en panne, et j'ai perdu le rapport que nous devions rendre aujourd'hui ! As-tu encore la dernière version sur ton disque ?
- Malheureusement j'ai installé hier un nouveau logiciel téléchargé sur le web, et depuis mon ordinateur ne fonctionne plus... »

Que peut-on craindre ?

- La perte de données suite à une défaillance matérielle ou humaine.
- L'indiscrétion ou l'atteinte volontaire à l'intégrité des données par une personne.
- La révélation des habitudes de navigation.
- L'attaque du système par un logiciel malveillant ou un pirate.

Comment sécuriser son espace de travail local ?

- En sauvegardant régulièrement ses données sur des supports amovibles ou distants.
- En limitant l'accès à son espace de travail et ses fichiers.
- En maîtrisant ses traces.
- En protégeant son système des logiciels malveillants.
- En identifiant les situations à risques.
- En étant capable de restaurer l'intégrité de son système.

Comment sécuriser son espace de travail distant ?

- En déposant ses fichiers dans un espace privé.
- En limitant tout risque d'usurpation d'identité (mot de passe complexe ; déconnexion de sa session ; etc.)

N.Denos – K.Silini
(cc) BY-NC-SA

La protection des données

La **confidentialité** est la garantie que l'information n'est accessible qu'aux personnes autorisées.

Pour lutter contre l'indiscrétion et favoriser la **confidentialité des données**, il est possible de protéger un fichier par un mot de passe :

- soit en l'enregistrant avec un mot de passe dans l'application ;

Au moment de l'enregistrement, les logiciels de bureautique permettent de définir un mot de passe qui sera requis pour ouvrir le document.

- soit en plaçant le fichier dans un environnement protégé par un mot de passe.

L'**intégrité** est la garantie que l'information n'a pas subi de modification par accident ou par malveillance.

Pour éviter toute modification, il est possible de protéger un fichier en écriture ; dans ce cas, il est possible d'ouvrir le fichier mais pas de le modifier à moins de l'enregistrer sous un autre nom.

Pour protéger un fichier en écriture à partir du système d'exploitation, cochez l'attribut « Lecture seule » dans les propriétés du fichier.

Pour éviter la destruction d'un fichier et favoriser **la confidentialité et l'intégrité des données**, il est possible de cacher le fichier :

- il faut d'abord cocher l'attribut "Fichier caché" dans les propriétés générales du fichier ;
- puis, paramétrer le gestionnaire de fichiers pour qu'il n'affiche pas les fichiers cachés.

Il ne s'agit pas d'une très bonne cachette car si on modifie les paramètres d'affichage du gestionnaire de fichiers, le fichier sera de nouveau visible ! Mais cela limite le risque de fausses manipulations. En particulier on peut cacher les fichiers systèmes dont la suppression accidentelle peut provoquer l'instabilité du système.

N.Denos – K.Silini
(cc) BY-NC-SA

La maîtrise des traces

Certaines traces mémorisées sur le disque dur de l'internaute lors de sa navigation sur le web pourraient être préjudiciables au respect de sa vie privée.

Les sites consultés et les fichiers téléchargés

On distingue :

- la liste des URL consultées (**historique**) ou sauvegardées (**signets**, **favoris** ou **marque-pages**) ;
- les fichiers que le navigateur télécharge pour l'affichage des pages web (**cache du navigateur**) ;
- les fichiers que l'internaute a téléchargés (**téléchargement**).

On peut constater que le temps d'affichage d'une page web (surtout s'il y a des photos) est beaucoup plus court à la seconde consultation : les fichiers étant déjà présents dans son cache, le navigateur n'a plus besoin de les télécharger.

Les préférences de navigation

Certains sites mémorisent à l'insu de l'usager des informations concernant ses habitudes de navigation.

Un *cookie* ou **témoin de connexion** est un petit fichier texte enregistré par le navigateur sur le disque dur de l'internaute lors de la consultation d'une page web.

Exemples :

- le cookie d'identification permet de naviguer entre les différentes pages d'un site en restant identifié ;
- le cookie de préférence permet de mémoriser la langue dans lequel la page doit s'afficher ;
- le cookie publicitaire permet de proposer des publicités ciblées.

Les cookies d'identification expirent après un certain laps de temps mais prenez l'habitude de vous déconnecter du service ou de fermer le navigateur si vous quittez le poste de travail.

Les mots de passe enregistrés

Pour chaque site demandant une identification, le navigateur peut enregistrer **avec son accord** le mot de passe de l'usager.

C'est pratique mais il faut être très vigilant : il est alors très facile d'usurper votre identité !

Attention, les mots de passe enregistrés peuvent être affichés en clair dans la plupart des navigateurs.

Pour éviter tout préjudice, il est possible :

- de configurer son navigateur pour une navigation privée (le navigateur ne retient aucune donnée des sites visités) ;
- d'effacer ses traces de navigation dans les options du navigateur en fin de consultation (historique, cookies, etc.) ;
- de refuser ou effacer l'enregistrement des mots de passe.

(cc) BY-NC-SA

Les logiciels malveillants

Un **pirate informatique** est une personne qui contourne ou détruit les protections d'un logiciel, d'un ordinateur ou d'un réseau informatique dans un but malveillant.

Un **logiciel malveillant** ou *malware* est un logiciel développé par un pirate dans le but de nuire à un système informatique.

Il existe différents types de logiciels malveillants.

« Un **virus** est un logiciel malveillant, généralement de petite taille, qui se transmet par les réseaux ou les supports d'information amovibles, s'implante au sein des programmes en les parasitant, se duplique à l'insu des utilisateurs et produit ses effets dommageables quand le programme infecté est exécuté ou quand survient un évènement donné. » sur FranceTerme (consulté le 16 août 2011)

On distingue :

- le **virus de boot** : il est chargé en mémoire au démarrage et prend le contrôle de l'ordinateur ;
- le **virus d'application** : il infecte un programme exécutable et se déclenche à l'exécution de celui-ci ;
- le **macro virus** : il infecte les documents bureautiques en utilisant leur langage de programmation.

« Un **ver** est un logiciel malveillant indépendant qui se transmet d'ordinateur à ordinateur par l'internet ou tout autre réseau et perturbe le fonctionnement des systèmes concernés en s'exécutant à l'insu des utilisateurs. » sur FranceTerme (consulté le 16 août 2011)

Contrairement au virus, le ver ne s'implante pas au sein d'un autre programme. Il se propage de façon autonome.

Les vers sont souvent conçus pour saturer les ressources disponibles ou allonger la durée des traitements. Ils peuvent aussi détruire les données d'un ordinateur, perturber le fonctionnement du réseau ou transférer frauduleusement des informations. Un ver peut produire des effets soit immédiatement soit de manière différée (à une date donnée, lors de la survenue d'un évènement ou par déclenchement d'une bombe programmée).

« Un **cheval de Troie** ou **Troyen** est un logiciel apparemment inoffensif, installé ou téléchargé et au sein duquel a été dissimulé un programme malveillant qui peut par exemple permettre la collecte frauduleuse, la falsification ou la destruction de données. » sur FranceTerme (consulté le 16 août 2011)

Le cheval de Troie ne se reproduit pas.

« Un **logiciel espion** ou *spyware* est un logiciel destiné à collecter et à transmettre à des tiers, à l'insu de l'utilisateur, des données le concernant ou des informations relatives au système qu'il utilise. » sur FranceTerme (consulté le 16 août 2011)

« Un **logiciel publicitaire** ou *adware* est un logiciel qui affiche des annonces publicitaires sur l'écran d'un ordinateur et qui transmet à son éditeur des renseignements permettant d'adapter ces annonces au profil de l'utilisateur. » sur FranceTerme (consulté le 16 août 2011)

Le logiciel publicitaire est souvent intégré ou associé à un logiciel gratuit ou à un partagiciel ayant un objet différent. Les logiciels publicitaires sont souvent assimilés à des logiciels espions.

En savoir plus...

Les virus, par Educnet

N.Denos – K.Silini
(cc) BY-NC-SA

La démarche de protection

Pour sécuriser son espace de travail, il faut éviter les comportements à risques et avoir un logiciel de protection installé sur sa machine.

Pour limiter les risques, il faut être vigilant...

- Ne pas ouvrir les fichiers dont on ne connaît pas l'origine : les fichiers exécutables (d'extension exe, sys, com, jar, etc.) peuvent infecter l'ordinateur et certains fichiers de bureautique peuvent contenir des macro virus.
- Ne pas croire qu'un fichier envoyé par un ami provient forcément de lui. Son système a pu être contaminé par un logiciel malveillant ou on a pu usurper son identité.
- Ne pas installer sur l'ordinateur des logiciels dont on ne connaît pas l'origine. Préférer les sites officiels ou reconnus pour télécharger une application.
- Mettre à jour régulièrement le système d'exploitation et les logiciels pour apporter des correctifs aux failles corrigées.

... et installer un logiciel de protection sur sa machine.

Quand un virus infecte un fichier, il place dans celui-ci un code spécifique : c'est la **signature virale**.

Un **antivirus** est un logiciel conçu pour protéger les ordinateurs des logiciels malveillants (virus, ver, cheval de Troie ou logiciel espion). Il possède une base de données de signatures virales et scanne les fichiers à la recherche de ces signatures dans leur code.

Un antivirus a trois principales fonctionnalités :

- une **protection résidente** ou veille, qui analyse tout nouveau fichier entrant ;
- un **scanner** qui peut analyser un support et y rechercher les logiciels malveillants ;
- un module de **mise à jour** (automatique) des signatures virales.

S'il détecte un fichier infecté, il offre plusieurs possibilités :

- il tente de le réparer en éliminant le virus ;
- il le place en quarantaine en l'empêchant d'agir :
- il supprime le fichier contaminé.

Un **pare-feu** ou *firewall* est un système permettant de protéger l'ordinateur des intrusions extérieures par le réseau. Il agit comme un filtre entre le réseau et l'ordinateur.

Le pare-feu a pour but de protéger les données sensibles (mots de passe, identités, données personnelles, etc.) contre les attaques de pirates qui cherchent à les dérober ou à installer des logiciels pouvant prendre le contrôle de l'ordinateur.

La plupart des logiciels antivirus ont également des fonctionnalités de pare-feu.

(cc) BY-NC-SA

La réparation

Les défaillances du système d'exploitation peuvent se manifester de plusieurs façons :

- l'ordinateur ne démarre pas ;
- l'ordinateur ne rend pas la main à l'usager suite à une de ses actions ;
- l'ordinateur s'arrête soudainement et un écran affiche un message qui tente d'expliquer le phénomène.

Quelle peut être l'origine du problème ?

On peut envisager plusieurs pistes :

- l'intégrité du système a été compromise lors de l'installation d'un nouveau logiciel ou d'une mise à jour du système ;
- le logiciel ou le système vient de rencontrer un bogue ou *bug*, c'est-à-dire une erreur dans le programme ;
- l'ordinateur est victime d'un logiciel malveillant ou de l'intrusion d'un pirate.

Comment réagir ?

Lorsque l'ordinateur ne parvient pas à démarrer le système d'exploitation, on peut choisir d'utiliser un système alternatif :

- une ancienne version du système ;
- un mode dégradé ou « sans échec » du système, qui ne lance que les parties du système les plus basiques ; on peut ainsi accéder de nouveau aux fichiers et à certains logiciels pour tenter de comprendre d'où vient le problème.

Pour cela il faut appuyer sur la touche indiquée lors de la toute première phase du démarrage : le lancement du BIOS.

La touche est souvent une touche de fonction, F2 par exemple. Attention, il faut être assez rapide !

Lorsque l'ordinateur ne rend pas la main, on peut :

- tenter d'utiliser le clavier pour forcer l'arrêt de l'application qu'on soupçonne d'être à l'origine du problème ;

Sous Windows, une combinaison de touche permet de voir la liste des applications en cours d'exécution, et d'en forcer l'arrêt.

- forcer l'ordinateur à redémarrer.

Il faut éviter tout choc électrique : on évite donc de débrancher l'appareil. On préfère appuyer longuement sur l'interrupteur qui sert à l'allumer : au bout de quelques secondes, cela coupe l'alimentation en douceur...

Lorsque l'ordinateur s'est arrêté soudainement, il faut d'abord suivre les recommandations qui s'affichent à l'écran au moment de l'arrêt :

- tenter de redémarrer l'ordinateur comme d'habitude ;
- si le problème se produit à nouveau, tenter de désinstaller la dernière application installée ;

Certains systèmes archivent les états successifs du système de façon à pouvoir restaurer facilement un état antérieur du système.

- en dernier recours, réinstaller complètement le système.

Lorsque les DVD d'installation ou de restauration du système d'exploitation ne sont pas fournis avec l'ordinateur, il est conseillé de les créer rapidement à l'aide de l'utilitaire prévu à cet effet.