Fiche pratique

Les risques de l'ordinateur

Après avoir présenté votre box, son contenu et plus particulièrement l'élément qui assure la protection de votre réseau contre les intrusions, il nous faut aller jusqu'au bout de la route, c'est à dire jusqu'à votre propre ordinateur.
Considérons un hacker, une personne qui s'introduit à votre insu sur votre réseau sans fil. S'il s'est donné la peine de cracker votre mot de passe c'est pour trois raisons possibles : pour le sport, pour la gratuité de l'accès à internet, pour vos données personnelles.

Pour le sport

Le but d'un hacker n'est pas de nuire. Son travail est très souvent lié à la sécurité, justement, et ainsi on peut être amené à lui demander d'évaluer, de tester ou d'auditer la sécurité d'un réseau. C'est un domaine tout à fait passionnant dans lequel les hackers se donnent un très grand plaisir. Il est envisageable que certains d'entre eux fassent des heures sup' pour tester la sécurité du réseau de leur voisin, pour s'entrainer, pour une recherche ou autre... Disons qu'il pratique un sport.

Pour la gratuité de l'accès

Même si nos abonnement sont aujourd'hui parmi les moins chers du monde, un certain nombre de personnes ne peut ou ne veut pas y souscrire pour différentes raisons et il apparaît parfois comme plus facile de se connecter au Wi-Fi d'un voisin. La procédure est enfantine et prend cinq minutes, parfois moins. Cela suppose néanmoins d'être en zone urbaine où le hacker est certain de pouvoir trouver un panel d'une dizaine de réseaux à attaquer. Statistiquement sur ces dix réseaux il est pratiquement certain de pouvoir se connecter sur l'un. Une fois connecté, cette personne ignorera parfaitement tout ce qui peut coexister sur le réseau pour peu qu'il ait un accès à internet. Il est très dangereux de penser que cela importe peu car vous êtes prêt à partager votre connexion, surtout si cela ne vous perturbe pas et que vous n'y êtes pas connecté, la nuit par exemple. Dans ce cas je vous conseille vivement de mettre en place un « hotspot » (réseau public ouvert) qui est nécessairement proposé par votre fournisseur d'accès au lieu de continuer dans cette situation. En effet ceci est très important car le fait de proposer un hotspot à partir de votre box établit en fait deux réseaux. L'un pour votre utilisation propre, et l'autre pour vos « invités ». L'un est prioritaire sur l'autre, ce qui fait que vous ne risquez pas de perdre l'usage de votre connexion si un trop grand nombre d'invités se connectent. La raison la plus importante de faire cela est que vous êtes juridiquement responsable de la partie de votre box que vous utilisez. Si vous mettez en place un hotspot vous créez une zone dans laquelle votre responsabilité n'est pas engagée. Supposez que votre « invité » utilise votre réseau pour se télécharger des images à caractère pédophile ou bien se livre à du téléchargement illégal, vous êtes juridiquement responsable (pénalement dans certains cas). Si la police mène une enquête sur un site qui héberge ce genre de contenu et que votre box est identifiée, vous serez considéré comme le fautif. Vous n'aurez absolument aucun moyen de le contester.
Suivez nos conseils dans les fiches documentaires pour apprendre à mettre en place un hotspot public ou la sécurité qui correspond à votre niveau d'exigence.

Pour le vol

Le dernier cas, non moindre, concerne vos propres données. Si le hacker est en fait un « cracker », un voleur de données informatiques et qu'il a pu s'introduire, même facilement sur votre réseau, il lui faudra peu de temps pour avoir accès à votre ordinateur et en parcourir le contenu.

Mots clés :

- WLAN
- Wi-Fi
- Hacker
- Cracker
- Pirate
- Sécurité
- Données personnelles
- Hotspot
- Responsabilité
- Mot de passe

Page suivante >

Il est impensable de laisser trainer un papier sur la table portant le numéro de sa carte de crédit accompagné de son code. Il en va de même avec ses fichiers informatiques. La plupart du temps, du fait d'avoir saisi un mot de passe protégeant son espace personnel des indiscrets de la famille, on se croit protégé. Il n'en est absolument rien et il faut véritablement considérer le mot de passe comme la moindre des protections. Posez-vous cette simple question : « Est-ce que mon mot de passe est dans le dictionnaire ou est-il composé uniquement de chiffres ? ». Si la réponse est oui, vous devriez en changer tout de suite car il faudra moins d'une demie-heure pour le trouver. D'une manière générale, pour accéder à vos fichiers, il suffit de posséder un CD-Rom sur lequel est installé GNU/Linux et on obtient l'accès complet aux fichiers de votre disque dur. Bon ceci est vrai quand on se trouve physiquement devant l'ordinateur, mais quand on est de l'autre côté du mur, les choses sont à peine plus compliquées car un scan des ports ouverts permet la plupart du temps de trouver une faille qui va donner accès à l'ordinateur. Comme en plus vous avez certainement configuré votre compte utilisateur en tant qu'administrateur de l'ordinateur, vous pouvez être sûr que votre pirate s'amusera à changer tous les réglages de l'ordinateur après vous avoir volé tous vos fichiers.

Allons bon, ce scénario catastrophe est un tantinet extrême mais il est tout a fait réaliste. Même s'il est difficile d'imaginer qu'un pirate en veut à nos fichiers, il est réaliste de dire qu'un éventuel pirate le fera en moins de cinq minutes (douche comprise). Les opérations permettant de se prémunir contre cela sont peu couteuses en temps et ne nécessitent pratiquement aucune connaissance en informatique, en tout cas rien que vous n'apprendriez sur Panoptinet !

Laissez-vous guider par nos fiches documentaires et nos fiches pratiques sur la sécurité pour faire les bons choix. Nous vous conseillons un certain nombre d'applications qui vous aident à vous protéger contre les virus, contres les vers, les intrusions etc... Mais n'oubliez pas que le seul remède efficace est vous-même et votre vigilance !

Repères :

Il peut être facile pour un hacker de s'introduire sur un réseau sans fil, tout dépend du degré de protection adopté par le titulaire de la connexion à internet. S'il y parvient, il peut s'en satisfaire, et ne pas devenir nuisible. Il peut aussi en profiter pour « surfer » gratuitement, sur tous les sites qu'il souhaite, même ceux au contenu illicite (pédopornographie, manifestation sectaire dangereuse, réseaux terroristes, etc.). Il a également la possibilité de télécharger illégalement des œuvres protégées par le droit d'auteur (musique, films, séries, etc.), toujours sans que le propriétaire du réseau s'en aperçoive. Enfin, il peut accéder à de nombreuses données personnelles (mails, mots de passe, données bancaires, etc.), et les réutiliser à sa guise.
Dans tous les cas, le titulaire de la connexion est responsable de l'usage qui en est fait, peu importe par qui. Si on ajoute à cela l'importance de sécuriser ses informations confidentielles, il n'y a pas à hésiter, il faut instaurer quelques règles de sécurité !