INTERNET MONITOR Security News 2005

EDITO

Bonjour chers internautes,
Dans cette édition du bulletin de sécurité 01/2005 vous trouverez une sélection de mes derniers tutoriaux (cours gratuits online) sur la "Sécurité PC&Internet". Le PC&Internet vous serons expliqués d'une manière transparente et non technique (VISUAL PC&INTERNET) !

SOMMAIRE

Il n'y a pas de problèmes, seulement des solutions.

Ensemble, nous trouverons la solution adéquate!

Mail : adcoet@pt.lu

Url : http://www.internetmonitor.lu

Copyright (FR) : C'est quoi le copyright?

Gust MEES

Le mot « copyright » vient bien entendu de l'anglais et traduit mot par mot, veut dire :
«Copy» = copie / « right » = droit, c. - à. – dire : avoir tous les droits sur les copies. En français on appelle le « copyright », propriété intellectuelle et il est symbolisé par le « © «.

Ceci signifie que nul n'a le droit de faire une copie de l'original exposé, sauf consentement de l'auteur !

Le copyright © et Internet ?

Sur Internet il est à la mode de copier et coller (copy&paste) tout ce qui bouge et personne ne se soucie de la légalité de cette action.

Pourtant, c'est défendu ! Même si vous surfez sur des sites Internet où il n'y pas de notifi-cation spéciale de copyright, sachez que le droit de la propriété intellectuelle est toujours présent !

Quand nous voulons copier une image et/ou un passage de texte sur un site Internet, nous devons, en principe, demander l'autorisation à son créateur et/ou auteur !

En principe, la plupart des sites Internet permettent le copier et coller (copy&paste) pour une utilisation dans l'enseignement et de l'éducation. Mais mieux est en tout cas de demander l'autorisation de son propriétaire, veuillez-en tenir compte pour votre phase de préparation des cours (temps de réponse de l'auteur).

Un petit courrier électronique (e-mail) à son auteur, concernant la demande de permission et le tour est joué, en principe. Rares sont ceux qui l'interdisent pour une application éducative.

En principe, les auteurs ne demandent que de mentionner la source de la copie.

Exemple pratique :

Si vous copiez une image et/ou un passage de texte de mon site Internet « Internet Monitor » http://www.internetmonitor.lu, veuillez mentionner à la fin de l'article et en dessous de l'image copiée « Source de l'article : http://www.internetmonitor.lu.

Sachez aussi, que si on vous attrape en flagrant délit et que l'on vous accuse devant un tribunal, vous risquez des sanctions assez graves ! Copier illégalement n'est pas un délis de mineurs (Kavaliersdelikt) !

Exemple : La loi Luxembourgeoise du 18 avril 2001, Recueil de législation / A - N 50, concernant le droit d'auteur :

Art. 1er. 1. Les droits d'auteur protègent les oeuvres littéraires et artistiques originales, quels qu'en soient le genre et la forme ou l'expression, y compris les photographies, les bases de don-nées et les programmes d'ordinateur.
Ils ne protègent pas les idées, les méthodes de fonctionnement, les concepts ou les informations, en tant que tels.

Art. 82. Toute atteinte méchante ou frauduleuse portée aux droits protégés au titre de la présente loi de l'auteur,des titulaires de droits voisins et des producteurs de bases de données constitue le délit de contrefaçon.

Est coupable du même délit, quiconque, sciemment, vend, offre en vente, importe, exporte, fixe, re-produit, communique, transmet par fil ou sans fil, met à la disposition du public et de manière géné-rale, met ou remet en circulation, à titre onéreux ou gratuit, une oeuvre, une prestation ou une base de données sans autorisation de l'auteur, du titulaire des droits voisins ou du producteur de base de données.

Est ainsi notamment coupable de ce délit, quiconque, sciemment, met à la disposition du public des phonogrammes, vidéogrammes, CD - ROM, multimédias ou tous autres supports, programmes ou bases de données réalisés sans l'autorisation des titulaires de droits d'auteur ou de droits voisins ou des producteurs de bases de données, ainsi que ceux qui reproduisent des oeuvres, des prestations ou des bases de données protégées pour les numériser, les mémoriser, les stocker, les distribuer, les injecter, et de façon générale, rendre possible leur accès par le public, ou leur communication au public.

Art. 83. Les délits prévus à l'article précédent seront punis d'une amende de 10.001 à 10 millions de francs (LUF).

La confiscation des ouvrages ou objets contrefaisants ou des supports contenant les contrefaçons, de même que celle des planches, moules ou matrices et autres ustensiles ayant directement

servi à com-mettre les délits visés à l'article précédent, sans condition quant à leur propriété, sera prononcée contre les condamnés, ainsi que celle de leur matériel de copiage, de numérisation ou d'injection sur les ré-seaux. Le jugement pourra de même ordonner la destruction des choses confisquées.

Art. 84. L'application méchante ou frauduleuse sur une oeuvre ou une base de données protégée du nom d'un auteur ou d'un titulaire de droits voisins ou d'un droit sui generis du producteur de base de données ou de tout autre signe distinctif adopté par lui pour désigner son oeuvre, sa prestation ou sa production sera punie d'un emprisonnement de 3 mois à 2 ans et d'une amende de 10.001 à 10 millions de francs LUF (approximativement entre 248 € et 248.000 €) ou de l'une de ces peines seulement.

Il en est de même pour l'ap-plication méchante ou frauduleuse à l'occasion de l'exploitation de la prestation d'un titulaire de droits voisins ou d'un producteur de bases de données ou sur le support qui contient cette prestation du nom d'un titulaire de droits voisins ou d'un droit «sui generis» des producteurs de bases de données ou de tout autre signe distinctif adopté par lui.

La confiscation des objets contrefaits sera prononcée dans tous les cas. Le juge pourra de même ordonner leur destruction.

Ceux qui, sciemment, vendent, offrent en vente, importent, exportent, fixent, reproduisent, communi-quent, transmettent par fil ou sans fil, mettent à la disposition du public et de manière générale, met-tent ou remettent en circulation à titre onéreux ou gratuit, les objets ou prestations désignés au premier alinéa du présent article seront punis des mêmes peines.

Le texte complet peut être trouvé à l'adresse suivante :
Texte législatif complet

http://www.cases.public.lu/documentation/legislation/luxembourgeois/droits_d_auteurs.pdf

Quelques recommandations :

Quand vos élèves créent leur propre « homepage » (Site Internet, web site), faites-en une petite introduction au « copyright » (propriété intellectuelle).

• Expliquez leurs qu'ils n'ont pas le droit de copier partout des images et des textes et les intégrer ensuite dans leur site Internet (homepage) !

• Expliquez leurs aussi qu'ils ne peuvent pas non plus publier des photos de personnes sur Internet sans avoir eu l'autorisation de ces personnes.

• Expliquez leurs aussi que publier quelque chose sur Internet veut dire qu'il y des millions de personnes partout au monde qui peuvent voir ces photos !

• Faites leurs montrer des sites Internet de législation où les amendes et punitions péni-tentiaires sont clairement expliquées et discuter avec eux sur ce phénomène du « co-py&paste » (copier et coller) !

• Expliquez leurs aussi qu'un jeune à partir de 13 ans en France (selon les pays cet age va-rie) est responsable de ses actes devant la législation !

• Expliquez leurs aussi que si ce n'est pas eux qui peuvent être responsabilisés, c'est leurs parents qui auront une « joie immense » pour se trouver devant le tribunal !

Pour vous donner une petite aide, un appui, veuillez trouver ci-dessous une sélection de liens se rapportant à la législation des N.T.I.C. :

Droit et Nouvelles Technologies (FR) : http://www.droit-technologie.org/3.asp

Droit du net (FR) : http://www.droitdunet.fr

Entre temps, pour ceux qui veulent se protéger contre le vol de leurs créations (textes et ima-ges), il existe pas mal d'outils, certains même gratuits et très performants !

Les techniques pour protéger les images et les textes :

1. Le « watermark » ou filigrane en français
2. Écrire du texte dans l'image
3. La stéganographie

Pour ne pas rentrer trop dans ces techniques, je conseille à ceux et celles qui veulent en savoir plus d'aller visiter les sites Internet suivants :

Stéganographie : http://lwh.free.fr/pages/algo/crypto/steganographie.htm

Watermark et/ou filigranes : http://lwh.free.fr/pages/algo/crypto/filigrane.htm

Visual Copyright ©

Comparez Internet avec un grand supermarché avec des milliards d'articles exposés à vos yeux. Dans un supermarché vous n'allez pas non plus voler les articles, en tout cas, j'espère pour vous !

Vous pouvez télécharger (download) le tutorial complet avec illustrations ä l'adresse suivante:

Téléchargement (PDF)
http://www.internetmonitor.lu/download/4.1.1._Le_copyright_07.02.2005..pdf

Éditorial : Morale et éthique sur Internet

Gust MEES

De plus en plus, Internet commence à devenir une poubelle du mauvais goût. Les blogs poussent comme des champignons, ce qui n'est pas négatif, bien au contraire. Les blogs nous ouvrent le chemin envers la communication, la liberté de nous exprimer, mais la liberté a son prix !

Fils RSS et blogs :

http://www.internetmonitor.lu/index.php?action=article&id_article=93408&id_rubrique=10031

Beaucoup de blogs sont abusés pour faire sortir la frustration de certaines personnes contre leur chef et/ou leurs collègues. Cette frustration se traduit par de la diffamation, des mots méchants, bref, la dignité des personnes est mise en cause ! Ces blogs sont de très mauvais goût et même contre toute morale, code éthique et aussi ils sont contre la loi !

Sachez que la dignité d'une personne est intouchable, aussi sur Internet !

Faites passer le mot à vos enfants, vos élèves, vos collègues de travail, votre famille et vos amis ! Les droits de l'homme sont protégés mondialement par des lois, même sur Internet ! Pour plus de renseignements, veuillez lire l'article suivant :

Visual PC :

http://www.internetmonitor.lu/index.php?action=article&id_article=119931

Sécurité PC & Internet : Nouvelles menaces, les « rootkits » :

Gust MEES

Le monde virtuel (Internet) n'arrête pas de nous étonner, dans le bien que dans le mal. Surtout les malware (virus, ver, troyen, etc.) poussent comme des champignons. La créativité des programmeurs de ces codes malicieux s'emble n'avoir pas trouvé de fin.
Une nouvelle sorte de ces malware est apparue, les « rootkits » !

C'est quoi les « rootkits » ?

Les « rootkits » sont bien connus depuis des années dans le monde de « UNIX » et de « LINUX » et font leur apparition officielle dans le monde de « WINDOWS » depuis mi-février 2005, selon un communiqué officiel de MICROSOFT et de la « RSA SECURITY ».

Ils s'intègrent en principe directement dans le cœur de WINDOWS, dans le « KERNEL » et ils se font passer comme étant des processus et services de WINDOWS. Même les scanneurs de malware (anti-virus, anti-troyen, etc.), ainsi que les « firewall » (pare-feu)

n'arrivent pas à détecter ces bestioles informatiques, dû au fait qu'ils ont développé une certaine intelligence.

Ils sont capables de se faire passer pour un service légitime de WINDOWS et de cette façon ils échappent au scan des anti-virus et des firewall !

Ils s'activent automatiquement dès démarrage du PC.

Leur rôle principal consiste à ne pas se faire révéler !

Quel est le but de ces « rootkits » ?

Le but en est bien de nature lucrative ($, €, £) ! Cette nouvelle sorte de malware ne veut rien d'autre que les autres malware aussi, faire du profit de la naïveté (non connaissance des risques de sécurité) des internautes !

En principe les « rootkits » peuvent être classés dans la catégorie « blended threats », une combinaison de « Troyens » plus « backdoor » et « keylogger ».

Seule différence avec les autres malware, ils ont été programmés soigneusement pour ne pas être détectés !

Ceci nous montre bel et bien, qu'il y a des professionnels cachés derrière cette nouvelle menace, la mafia informatique, des groupes de criminels bien organisés !

La priorité des programmeurs des « rootkits » est de ne pas se faire repérer, une sorte de code éthique !

Ces programmes (logiciels et scripts) peuvent « dormir » et attendre jusqu'à ce qu'ils deviennent « réveillés » par leur programmeur et ainsi envoyer toutes vos données secrètes à leur(s) programmeur(s) !

De cette façon, ces malfaiteurs auront accès à vos comptes bancaires et à toutes vos transactions faites par Internet !

Comment nous protéger et avec quoi ?

La seule chose que nous pouvons faire est de nous munir d'un anti-virus, d'un firewall et d'être à jour avec les updates (patches / mises à jour) de notre système d'exploitation (WINDOWS, MAC OS, LINUX) !

Un logiciel (programme) anti-troyen comme « A squared » de chez « EMSISOFT » http://www.emsisoft.net est fortement à recommander !

Ce logiciel (programme) en version payante de 39,95 € est pourvu d'un „IDS ". Un « IDS » surveille tous les processus dans le système d'exploitation. Le Gardien d'arrière-plan de a-squared empêche et bloque les fichiers dangereux d'arriver sur votre PC bien avant qu'ils ne deviennent actifs. Pour cela, il utilise une nouvelle technique et unique dans le monde entier qui s'appelle "analyse du comportement des programmes" (IDS) qui vous donne immédiatement une alarme, aussitôt qu'un programme démarré fait quelque chose de dangereux.

Comportement de l'analyse

Contrairement aux heuristiques traditionnelles, qui recherchent des fichiers contenant des routines nuisibles sur le disque dur et qui fournissent une analyse approximative, si un fichier est dangereux ou non, a² lui surveille directement le comportement des programmes actifs dans le système.

2. Que détecte-t-il ?

a² est actuellement entraîné pour trouver les types de Malwares suivants:

• Vers Emails
• Backdoors (Porte dérobée)
• Backdoors avec Reversed Connection Logic (LAN Bypass)
• Spywares/Adwares
• HiJackers
• Dialers
• Rootkits

Fonctionnement de l' »IDS » à l'adresse suivante : http://www.emsisoft.net/fr/software/ids/

Pour l'instant (04.05.2005.) il n'existe pas de programmes (logiciels) actuels qui puissent être capables de détecter et d'éradiquer ces bestioles informatiques.

Selon le magazine informatique professionnel allemand « COM ! », édition 06/2005, page 8, http://www.com-magazin.de , il existe des logiciels (programmes) qui détectent ces « rootkits ».

Il s'agit de deux logiciels :

1. STRIDER GHOSTBUSTER de MICROSOFT
2. ROOTKIT-REVEALER de SYSINTERNALS

http://research.microsoft.com/rootkit/

http://www.sysinternals.com/ntw2k/freeware/rootkitreveal.shtml

Malheureusement ces deux logiciels arrivent à détecter ces « rootkits », mais sont incapables de les éradiquer !

Nos statistiques : TOP 10

Gust MEES

Les rubriques TOP 10 et les articles les plus lus au 23.04.2005.
Les statistiques sont organisées par tableaux, contenants des hyperliens (links) pointants vers les articles.

De cette façon vous avez la possibilité de visiter ces sites pour vous faire une idée (opinion) des intérêts de nos visiteurs.

Les rubriques TOP 10

Rubriques
Visites

01.) Tutoriaux
3474

02.) Security News (FR)
2663

03.) MICROSOFT News (FR)
1470

04.) MAUSI
2087

05.) Éditorial
2029

06.) Freeware
1355

07.) MICROSOFT News (DE)
1304

08.) Spam (FR)
1194

09.) Notifications Virus (FR)
1168

10.) Protection des mineurs
1082

Les 3 premières catégories en détail :

01.) Tutoriaux

C’est quoi un port ?
360

Troyens, Trojans, Chevaux de TroieCet article est aussi publié sur Veille citoyenne (BE) et a été lu 1659 fois !
332

Spyware (FR)
301

02.) Security News (FR)

Les Top-News sur la Sécurité en français
164

Démantèlement d’un réseau ZOMBIES
144

Modification logiciels anti-virus
134

3.) MICROSOFT NEWS (FR)

Nouvelles failles MSN MESSENGER,OFFICE et WINDOWS
446

8 failles critiques
135

MICROSOFT publie un correctif...
134

Spam (FR) : Votre PC est-il un «zombie» à louer?

Gust MEES

Plusieurs virus poursuivent de plus belle leur sale besogne: transformer les PC qu'ils infectent en «zombies» exploitables à distance par des polluposteurs ou par des pirates informatiques, ceci à l'insu des propriétaires de PC qui peuvent ainsi se retrouver complices de malfaiteurs.

En sécurisant le PC ceci n'arriverait pas!

Les PC infectés transformés en «zombies» seraient légion sur Internet; selon des évaluations parmi les plus conservatrices, environ 500.000 ordinateurs sous Windows, préalablement infectés par un ver informatique ou un cheval de Troie, seraient ainsi dans l'attente d'instructions de polluposteurs ou de pirates, tandis que d'autres sources soupçonnent que le nombre de ces «zombies» approcherait plutôt deux millions ou même davantage.

Les «zombies» se multiplient

Avec la publication de ses dernières statistiques, la firme anti-pourriel Postini annonce que plus d'un courriel sur deux (53%) peut maintenant être bloqué avant même que le contenu des messages soit sondé. Postini explique que le comportement des adresses IP à l'origine des courriels est d'abord analysé et que dans l'éventualité où son système détermine que les messages résultent de l'activité d'un polluposteur, notamment via des PC «zombies», ceux-ci sont immédiatement bloqués.

Postini précise que cette proportion n'était que de 35% à l'automne 2003 et que la hausse récente à 53% est «due en partie à l'augmentation d'activité provenant de PC domestiques compromis qui ont été transformés en "zombies" pour expédier des courriels commerciaux non sollicités». Comme on aurait pu le prévoir, l'entreprise indique également que l'étude parallèle des PC qui expédient des vers informatiques permet d'atteindre une précision encore meilleure dans ce blocage préventif.

Réseaux de «zombies» à louer

De plus, il existerait un marché noir pour exploiter ces ordinateurs «zombies» qui, groupés en réseaux de 10.000 à 30.000 machines (les botnets), pourraient être loués à partir de 100 $US de l'heure, comme l'indiquait notamment un article récent de l'agence de presse Reuters.

Parmi les clients potentiels pour ces botnets, on pourrait par exemple citer les cas de maîtres chanteurs qui menacent d'attaquer des commerces en ligne et exigent le paiement d'une «protection», de fraudeurs qui veulent propager discrètement des arnaques par courriel de type «phishing» ou de simples polluposteurs à la recherche d'anonymat pour éviter les poursuites judiciaires.

Guérir les «zombies»

Qui sont les propriétaires de ces PC «zombies»? La plupart du temps, ce sont des internautes qui ont cédé à la curiosité d'ouvrir un fichier joint arrivé dans un courriel au titre alléchant et, dans tous les cas, des gens qui ne possèdent pas de logiciel antivirus à jour en dépit du fait que certains sont offerts gratuitement, notamment Avast, AVG et l'outil de balayage en ligne de Bitdefender.
Source de l'article: BRANCHEZ-VOUS (CA)

Éditorial : La vigilance avant tout

Gust MEES

**Je viens d'analyser les statistiques de visite de notre web magazine „Internet Monitor" et c'est avec une grande joie que j'ai pu constater que les tutoriaux, qui sont d'ailleurs gratuits, sont en tête du peloton avec un grand écart sur les autres rubriques.

**
**TOP 10 Rubriques

**

Ceci me démontre bel et bien que mon choix de vous présenter et d'écrire des tutoriaux pédagogiques gratuits sur la Sécurité PC&Internet est bien fondé ! Et c'est bien comme ça. Payer pour des cours se Sécurité PC&Internet, c'est pas logique ! Nous, payer pour le non professionnalisme et les conneries des autres, certes pas !

C'est d'ailleurs pour cette raison que le volet « Tutoriaux » sera élargie encore beaucoup plus dans le futur, bien entendu « gratuitement » !

D'ailleurs, je suis d'avis que l'éducation devrait être gratuite, au moins l'éducation à la Sécurité PC&Internet ! C'est pour cette raison, que la rubrique « Tutoriaux » sera élargie avec des « Trucs et Astuces » et aussi avec des idées pour nos tout jeunes (4 ans et plus) !

La sensibilisation aux dangers de l'Internet commence dès le plus jeune age (4 à 5 ans) et croyez moi, c'est bien possible ! Des visites sur Internet, ensemble avec ma nièce (4 à 5 ans) l'ont bien démontré.

Lui expliquant à chaque fois, dès connexion à Internet qu'il faut regarder que l'antivirus est activé, elle l'a compris. Maintenant, elle a presque 6 ans et chaque fois que nous surfons ensemble, elle me demande déjà avant de nous brancher sur Internet : « Gusty, est-ce que tu as activé le *nantivirus* » ?

Elle est devenue vigilante entre temps, certes elle ne comprend pas tout ce qui est derrière la technique, mais le fait d'y penser à faire attention quand nous nous connectons à Internet, c'est cette action qui est la plus importante et elle l'a compris (4 ½ ans)!
La vigilance, cela s'apprend par l'intermédiaire de l'éducation!

Pour revenir à la vigilance ; je vous proposerais prochainement une nouvelle rubrique, appelée « Editors choice ».

Cette rubrique contiendra des articles et tutoriaux qui seront relancés, c. - à. - dire :
Périodiquement j'analyserais les statistiques et je fais mon choix sur des articles et tutoriaux, qui à mon avis, n'ont pas été pris au sérieux assez comme je me l'imaginais. Ces tutoriaux et articles sont quand même très importants.

C'est pour cette raison qu'ils seront publiés encore une fois (relancés) ! Notez toute fois, que vous avez la possibilité d'exprimer votre opinion à ces articles. Ceci pour mieux vous servir. En dessous des articles, vous voyez « Ajouter un commentaire », profitez en pour dire ce que vous pensez de la qualité de mes tutoriaux !

Vos commentaires me diront si mes tutoriaux sont adaptés à votre

type d'apprenant ou si je devrais les présenter autrement. Avis aux amateurs.

Editors Choice : Est-ce que votre PC est sécurisé ?

Gust MEES

Afin de vous faciliter la tâche pour voir si votre PC est bien sécurisé, j'ai créé un petit questionnaire avec tutoriel. essayez de répondre le plus soigneusement que possible les questions et vous aurez la réponse.

EST-CE QUE VOTRE PC EST SÉCURISÉ ?

Veuillez répondre soigneusement aux questions posées et à la fin de ce questionnaire vous y trouverez un tableau avec des conseils à suivre.

Après avoir coché toutes les cases correspondantes, veuillez cliquer le bouton *Imprimer cette page*. restez en ligne (online), vérifiez et comparez vos résultats avec le tableau en bas de page.

Pour les coïncidances des réponses avec le tableau, veuillez suivre les conseils et les liens y présents dans le tableau pour vous éclaircir sur la matière !

Je vous souhaite bon apprentissage et une bonne volonté à devenir et à apprendre de devenir *vigilant* et *responsable*!

1. Est-ce que vous utilisez un logiciel (programme) anti-virus?

Oui

Non

2. Si OUI, est-ce que vous l'avez actualisé (update/maj) endéans la dernière semaine ?

Oui

Non

3. Que faites vous lors réception d'un

courrier électronique (email) non demandé et d'une personne inconnue, contenant une pièce jointe:

A) Demander l'expéditeur ce qu'il m'a envoyé ?

B) Effacer (Jeter à la poubelle) ?

C) L'ouvrir et regarder son contenu ?

4. Est-ce que vous avez entendu parler ou lu d'une vulnérabilité et *security patch* endéans les 6 derniers mois?

A) Oui, j'ai lu des informations sur une vulnérabilité et d'un patch (rustine) de sécurité.

B) Oui, j'ai lu des informations concernant soit la vulnérabilité ou le patch, mais pas les deux.

C) Non, je n'ai eu aucune information concernant la vulnérabilité, ni le patch de sécurité endéans les derniers 6 mois.

Où puis-je avoir ces informations ? ---> Internet Monitor + MICROSOFT UPDATE

5. Est-ce que vous utilisez un firewall (pare-feu)?

A) Oui

B) Non

C) Ne sais pas/Suis pas sûr ?

6. Est-ce que vous utilisez du P2P (échange de fichiers) sur Internet ?

A) Non, je n'utilise pas de P2P (échange de fichiers).

B) Oui, j'utilise le P2P (échange de fichiers) et je connais les services proposés.

C) Oui, j'utilise le P2P (échange de fichiers) mais je ne connais pas les services proposés ou ne suis pas sûr.

7. Quand vous n'utilisez pas Internet est-ce que vous désactivez la connexion ?

Oui

Non

8. Les mots de passe (passwords) doivent être très complexes et contenir minimum 8 digits. Ils doivent contenir des nombres mélangés avec des majuscules et des minuscules. Est-ce que vous utilisez vos mots de passe avec :

A) Nombres et majuscules ainsi que des minuscules mélangés ?

B) Seulement 2 des 3 ?

C) Soit l'un ou l' autre ?

9. Quand est-ce que vous aviez sauvegardé pour la dernière fois un fichier important (Back up)?

A) Endéans la dernière semaine

B) Endéans le dernier mois

C) Jamais

10. Est-ce que vous utilisez un logiciel (programme) anti-troyen ?

Oui

Non

C'est quoi un anti-troyen ?

11. Est-ce que vous utilisez un logiciel (programme) anti-spyware ?

Oui

Non

C'est quoi un anti-spyware ?

12. Est-ce que vous téléchargez toujours les dernières mises à jour (MAJ / Updates) de chez MICROSOFT ?

Oui

Non

Adresse des updates à télécharger : MICROSOFT UPDATE

13. Est-ce que vous connaissez tous les mots suivants: Phishing, Hijacking, Virus, Troyen, Spyware, Malware, etc.

Oui

non

```
function printPage() {
if(document.all) {
document.all.divButtons.style.visibility = 'hidden';
window.print();
document.all.divButtons.style.visibility = 'visible';
} else {
document.getElementById('divButtons').style.visibility = 'hidden';
window.print();
document.getElementById('divButtons').style.visibility = 'visible';
}
}
```

Questions

Si votre réponse est :

ActionsVeuillez cliquer les liens (links) dans les cellules pour recevoir plus de renseignements !

Question 01

Non

Un logiciel (programme) anti-virus est obligatoire !Veuillez lire aussi : Visual PC et aussi Sécurité PC&Internet

Question 02

A ou C

Comment actualiser l'anti-virus Norton Internet Security ? Page 1/2 Page 2/2

Question 03

A ou C

Ne jamais ouvrir de courrier électronique (email) de personnes inconnues. Surtout pas des pièces jointes (attachments) !

Question 04

B ou C

Inscrivez vous à notre Newsletter Vous recevrez gratuitement les notifications des *patches de sécurité* ainsi que la notification de nouveaux tutoriaux.

Question 05

B ou C

Un Firewall (pare-feu) est obligatoire !

Question 06

B ou C

45 % des fichiers de *KAZAA* sont infectés ! Lire aussi les articles suivants : KAZAA logiciel espion le plus menacant et KAZAA 45%

Question 07

Non
Vous exposez votre PC à des risques inutiles !

Question 08
B ou C
Vous facilitez les tâches pour le Hacker !

Question 09
B ou C
Au cas d'un *Crash* ou d'une infection virale, vos données sont perdues !

Question 10
Non
Votre PC est vulnérable ! Installez a2

Question 11
Non
Vous êtes espionnés et vous allez recevoir du courrier non sollicité (SPAM) sans savoir pourquoi. Installez un logiciel *anti-spyware*.

Question 12
Non
Votre PC est déjà infecté ou le sera très prochainement !

Question 13
Non
Veuillez lire mes tutoriaux (Cours gratuits en ligne) !

Veuillez lire aussi les articles suivants comme complément :

CASES LuxembourgVers et Virus
CASES LuxembourgChevaux de Troie
CASES LuxembourgPerte de données

La bonne procédure pour avoir un PC sécurisé au maximum avec un minimum d'investissement :
Guide pratique de la Sécurité

Éditorial : Visual PC & Internet

Gust MEES

Le monde virtuel (Internet) nous réserve de plus en plus des surprises avec de nouvelles arnaques. Plus rien n'est encore sûr et chaque jour nous révèle de nouvelles vulnérabilités, même dans des systèmes et logiciels qui, il y a un mois, étaient encore promis les meilleurs et les plus sécurisés !

Plusieurs navigateurs souffrent d'une faille permettant l'hameçonnage

Brèches critiques dans Mozilla et Firefox

La « mafia informatique » travaille très vite et elle profite de la non vigilance et non connaissance des internautes (nous même) ! Ce ne sont pas seulement les logiciels de sécurité qui peuvent aider à sécuriser et à protéger notre PC, mais d'abord il faut savoir les utiliser aussi !

Eh bien oui, c'est nous, les utilisateurs du PC et de l'Internet, qui sont responsables et qui le seront encore plus responsabilisés dans le futur ! Une solution « CLIC », comme avec une télécommande à la maison, n'existe pas et ne sera jamais inventée pour garantir une sécurité à 100%. De toute façon, une sécurité à 100% n'existe pas et est illusoire !

Ce nouveau mass média (PC&Internet) n'est pas seulement domptable avec la technique, mais surtout avec de la vigilance et des connaissances nécessaires pour se servir des logiciels (programmes) de sécurité !

C'est à nous d'apprendre à nous servir de ces logiciels et d'apprendre à devenir vigilant !
Apprendre et vigilance ?

Eh bien oui, nous n'avons pas le choix. Il ne suffit pas d'utiliser cet outil technique et de croire que tout fonctionne à merveille, mais ce « joujou » (Internet), qui n'en est pas mais que la plupart des gens croient que s'en est un, est intelligent et il grandit à une vitesse incroyable.

C'est un « joujou » qui vit, c'est un monde virtuel pour lequel nous sommes responsables. C'est nous, qui nous copions dans ce monde avec tous nos mérites et nos défauts !

Internet est le miroir de la morale de notre société ! Cela vous fait penser et réfléchir ? J'espère bien, peut être alors, vous comprendrez comment Internet fonctionne vraiment !?

Visualisation pratique :

Si vous avez attrapé un virus (grippe) et que vous ne restez pas à la maison et que vous ne vous soignez pas, vous infectez aussi votre entourage avec le virus, les autres personnes deviendront aussi malades.

Si votre PC a attrapé un virus, vous infectez aussi les autres internautes partout au monde et une épidémie virale informatique se propage (Internet ne connaît pas de frontières, ni de distances)

Internet est un produit « vivant » de la technique qui réunit toutes nos connaissances et l'expression de nos caractères et émotions !
C'est nous tous qui faisons « vivre » Internet !

Internet est un produit technique, qui est dépendante de nos actions et réactions. Quand nous publions des articles sur un site Internet (Web site / Homepage), quand nous agissons sur un forum avec des questions et/ou des réponses, nous devons être conscients que toute personne, partout dans le monde et ayant une connexion Internet et un PC, a la possibilité de voir nos idées et de réagir, ceci même instantanément !

Le monde réel, nous ne savons pas le saisir directement [sauf par les mass média] (Télévision, radio et journaux), seulement le toucher et le sentir. Internet, le monde virtuel nous ne savons pas le saisir, ni toucher et sentir (puisque c'est un mass média).

Ce que les deux mondes ont en commun, est la communauté (nous tous), qui les font vivre. La collectivité, la communauté, elle commence par nous même, par l'individu. Plusieurs individus forment une communauté.

Déjà nos ancêtres, (préhistoire) vivaient en communauté, cela leur permettait de mieux survivre.
De nos jours, nous vivons plutôt selon une « politique des coudes ».

Mais même les animaux nous démontrent bel et bien, que vivre en communauté et surtout avec un esprit de communauté (vivre pour la communauté) est très bien possible et qui fonctionne à merveille.

De très beaux exemples de communautés qui vivent en parfaite harmonie et qui travaillent pour la communauté se trouve dans la nature. Prenez par exemple les fourmis et les abeilles. Comme vous pouvez le constater, les animaux sont capables de le faire. Nous les êtres humains présumons être supérieur aux animaux, est-ce vrai ?

Si vous dites « oui », alors démontrez-le ! Pensez avec un esprit de collectivité et de communauté !

Si la communauté se porte bien, nous allons nous sentir bien aussi, car nous faisons part de la communauté !

Internet, comme déjà décrit, est un produit « vivant » de la technique ! À visualiser comme un « enfant » qui sera éduqué par des millions de personnes en même temps, avec des traditions et langues différentes, avec des mentalités différentes et ceci en temps réel.

« L'enfant » Internet,

Compilation Sécurité PC&Internet : Compilation Sécurité PC&Internet

Gust MEES

Le PC et Internet ont créé un nouveau mass média, une base de données inépuisable, grandissante à chaque seconde. Ce mass média nous ouvre le monde de la communication et de l'information.
Pour tout ce qui est nouveau, il nous faut un certain temps pour nous habituer, nous familiariser, apprendre à nous servir de cette nouvelle technologie.
Toute nouvelle technologie requiert aussi un entretien technique

et des consignes de sécurité !

Le PC et Internet n'y font pas exception !

Pour vous faciliter la tâche, j'ai créé ce tutoriel pour voir plus clair.

Étant donné qu'il y a une circulation impressionnante de malware (code malicieux, Virus, Ver, Dialer, Troyen, Spam etc.) sur Internet, nous devons sécuriser notre PC.

Aucun système d'exploitation (OS) de nos jours n'est assez sécurisé par sa version d'installation d'origine. Ni le MAC, ni LINUX, ni les PC avec WINDOWS.

D'ailleurs il ne le sera pas si tôt dans le futur. L'évolution rapide des malware (virus, vers, troyens, etc.) progresse et une solution globale de protection n'est pas encore en vue !

Plus aucun système d'exploitation (OS) n'est encore sûr de nos jours !

La vulnérabilité du système d'exploitation de WINDOWS ® est bien connue, mais aussi les autres sont vulnérables !

Veuillez vous renseigner aux liens suivants :

LINUX :

Vulnérabilités LINUX MAC :

Vulnérabilités MAC C'est pour cette raison que nous devons nous aider nous même !

Mais comment sécuriser notre PC ?

Rappelons-nous un peu les vieux proverbes qui disent :

" Danger connu est danger vaincu. " En allemand "Gefahr erkannt ist Gefahr gebannt." En anglais "Forewarned is forearmed."

Ceci nous indique bien que si nous connaissons les dangers, nous deviendrons automatiquement plus vigilants et le pourcentage que nous attraperons une de ces malware va déjà être réduit.

C'est pour cette raison qu'il vaut mieux nous informer régulièrement ! Je vous conseille de vous abonner au Newsletter de notre Internet Monitor à l'adresse suivante :

Internet Monitor http://www.internetmonitor.lu

Si maintenant, après avoir acquis ces connaissances des dangers, nous installons encore des logiciels de sécurité sur notre PC, nous serons sécurisés au maximum.

Mais veuillez noter quand même qu'une sécurité à cent pourcent (100%) n'existe pas et est illusoire !

Comme nous sommes maintenant conscients qu'il y a des dangers existants, essayons de nous protéger avec les logiciels (programmes) existants sur le marché.

La plupart d'entre eux est même gratuite (Freeware), mais très performant et même dépassant les produits commerciaux (payants) !

Ce qu'il nous faut installer comme logiciels (programmes) pour sécuriser notre PC et autres précautions :

1. Un anti- virus commercial ou Freeware
2. Un Firewall (pare-feu)
3. Un anti- troyen
4. Un anti- dialer
5. Un anti- spyware
6. Installer régulièrement les updates (patches) de chez MICROSOFT et aussi MAC et LINUX ! Nul n'est parfait !
7. Respecter la Nétiquette et la Chatiquette

Autres précautions à prendre :

Ne jamais ouvrir du courrier électronique (email) de personnes inconnues, surtout pas les pièces jointes (attachments) !

Nouvelle variante du PHISHING :

Nouvelle variante du PHISHING

Ne jamais ouvrir de courrier électronique (email) vous demandant de saisir à nouveau vos données (Banques, Ebay, etc.) Danger de Phishing !

Il existe deux sortes d'attaques :

1. Attaques par courrier électronique
2. Attaques dues à un système d'exploitation non mis à jour (Windows updates)

Lire aussi :

Phishing, le nouveau fléau d'Internet

Phishing, le nouveau fléau d'Internet

Les arnaques bancaires se multiplient dans le monde

Les arnaques bancaires se multiplient

Description de fonctionnement des programmes (logiciels) différents

L'anti-virus

L'anti-virus est le système immunitaire contre les épidémies virales informatiques de notre PC. Quand il y en a pas, nous sommes vulnérables et nous serons infectés tôt ou tard !

Veuillez aussi lire l'article suivant :

Un PC sans protection ne survivrait que 20 minutes sur Internet

Un PC sans protection ne survivrait que 20 minutes sur Internet

Une fois infectés, nous infecterons aussi les autres internautes. Comme Internet fonctionne selon le principe de la communauté, nous devons faire attention aussi aux autres internautes (utilisateurs d'Internet), les respecter. Dès que nous sommes connectés à Internet, nous surfons ensemble avec des millions d'autres internautes !

Lire aussi :

Visual PC

Visual PC http://www.internetmonitor.lu/pcsecurity

Comprendre Internet

Comprendre Internet

Le PC, Internet et son utilisation

Le PC, Internet et son utilisation

Les dangers sur Internet en chiffres

Les dangers sur Internet en chiffres

L'anti-virus est le vaccin pour notre PC. Il existe différents fabricants de logiciels anti-virus, dont voici ci-dessous une liste des plus renommés et performants :

Les logiciels (programmes) présentés ici sont des versions contenants un anti-virus et firewall (pare-feu) dans un seul package.

Norton Internet Security

McAfee

Trend Micro PC Cillin

Bitdefender

AVG Anti Virus (Freeware / Gratuit)

Actuellement, un des plus performants (selon les tests de magazines professionnels PC) est Norton Internet Security, que vous pouvez trouver à l'adresse suivante :

Norton Internet Security http://www.symantec.com

Les autres logiciels mentionnés ci-dessus sont pareils, ils ont aussi déjà un Firewall (pare-feu) intégré.

Lire aussi Firewall et Anti-Virus :

Firewall et Anti-Virus http://www.webwizardbiz.com/tutorials/firewalls/

Le Firewall (pare-feu)

Le Firewall (pare-feu) est le système anti-intrusion (système d'alarme) pour notre PC. Il bloque le trafic des données non désirées entrantes et sortantes sur notre PC.

À voir comme un portier qui contrôle le va et vient.

On appelle les logiciels (programmes) Firewall aussi des Desktop Firewall.

Une autre sorte de Firewall (pare-feu) est le Hardware Firewall. Celui-ci est branché par câble à l'ordinateur ou il est déjà intégré dans les nouvelles générations de Router.

Le Router gère le trafic des données entre le serveur et les PC différents.

En version Freeware (GRATUIT) il existe aussi ZONE ALARM PRO qui est très performant et selon les tests de magazines PC professionnels, actuellement le meilleur (01.01.2005.)

ZONE ALARM http://www.zonelabs.com

C'est quoi un Troyen (Cheval de Troie) ?

C'est quoi un Troyen (Cheval de Troie) ? Un programme (logiciel) très efficace, qui éradique ces bestioles informatiques (malware/ troyens, virus, vers, dialer, etc.) et qui nous protège aussi contre ceux-ci est a2 (a squared) de Emsisoft.

Ce logiciel (programme) est multi langues, très efficace et très facile à utiliser (aucune configuration).

Vous trouverez un tutoriel (cours gratuit online) à l'adresse suivante :

Comment installer et s'en servir de a2

Comment installer et s'en servir de a2

L'anti-spyware

Des programmes espions, appelés aussi mouchards ou spyware s'installent sur notre PC à notre insu (sans que nous nous en apercevons).

Ces programmes espionnent nos habitudes de surf sur Internet et envoient les résultats obtenus de leur enquête à leur programmeur, lequel revend ces informations à des polluposteurs (envoyeurs de Spam) ou et à des firmes non sérieuses faisant de la publicité forcée sur Internet.

L'effet que cela fait est, que nous serons bombardés par des fenêtres pop up (fenêtres surgissant soudainement sur l'écran), montrant de la publicité sur des articles qui pourraient nous intéresser.

On appelle ceci aussi de la publicité ciblée.

Une liste de logiciels (programmes) qui nous protègent contre ces espions et qui les éradiquent aussi, peut être trouvée à l'adresse suivante :

liste de logiciels (programmes) qui nous protègent contre ces espions

En plus, un tutoriel (cours gratuit online), comment installer ces programmes et comment s'en servir, peut être trouvé aux adresses suivantes :

C'est quoi les Spyware ?

C'est quoi les Spyware ?

Comment installer et se servir de Spybot Search&Destroy ?

Comment installer et se servir de Spybot Search&Destroy ?

Autant de programmes (logiciels) pour sécuriser notre PC ?

Eh bien oui, malheureusement ! Mais la tendance (trend) va vers des logiciels, (programmes) lesquels intègrent toutes les fonctions mentionnées dans cet article dans un seul logiciel (programme).

Mais, tant qu'ils ne sont pas encore disponibles sur le marché, il nous faudra vivre avec cette situation et installer ces différents logiciels (programmes) !

Pour vous faciliter la tâche, j'ai créé un tutoriel, le Guide pratique de la sécurité, lequel vous trouverez à l'adresse suivante et que vous pouvez aussi télécharger (download) :

Guide pratique de la sécurité http://www.webwizardbiz.com/tutorials/guidesecurite/

Essayez de suivre ce tutoriel à la lettre et consacrez +/- 15 à 20 minutes par week-end pour votre sécurité et celle des autres.

Si tout internaute aurait installé au moins un anti-virus et un Firewall (pare-feu), Internet serait déjà plus sûr.

Une étude a démontré que 80% du Spam serait généré par des PC

non sécurisés, à voir, des PC Zombies.
Votre PC est-il un ZOMBIE ?
Votre PC est-il un ZOMBIE ?
http://www.internetmonitor.lu/index.php?action=article&id_article=67428
Nos responsabilités dans Internet :
Nos responsabilités dans Internet
http://www.internetmonitor.lu/index.php?action=article&id_article=67346
Je vous conseille de lire les articles mentionnés ci-dessus, afin de mieux comprendre le sérieux de la sécurité pour nous tous !
FAQ's (Frequently asked questions) :
Mais j'ai installé WINDOWS XP et le SP2, je suis sécurisé ?
Réponses :
1) Faux. D'abord le Firewall (pare-feu) de WINDOWS XP ne bloque que les données non désirées entrantes et pas les données sortantes !
2) Il faut quand même faire les updates de chez MICROSOFT régulièrement
3) Il faut quand même installer en plus les programmes (logiciels) anti-malware mentionnés en début de cet article !

Comment nous informer sur les nouvelles menaces ?
Vous avez la possibilité de vous inscrire au Newsletter (Lettre d'information) de mon site Internet, l'Internet Monitor à l'adresse suivante :
http://www.internetmonitor.lu
Il suffit d'inclure votre adresse e-mail et cliquer sur inscrire. Ensuite vous serez informés régulièrement sur des nouvelles menaces, sur des nouveaux produits, sur des tutoriaux (Cours gratuits
On line) concernant la sécurité PC&Internet, des trucs et astuces sur le PC&Internet, des téléchargements gratuits etc.
L'Internet Monitor est un site Internet reconnu d'utilité public et professionnel. Il est d'ailleurs aussi répertorié dans le Guide des meilleurs sites Internet et répertorié aussi chez lamoooche.com, un catalogue professionnel de syndication de contenu XML (RSS, ATOM FEED) !
http://www.bonweb.com
http://www.lamoooche.com

En plus notre Internet Monitor est partenaire officiel du Ministère de l'Économie Luxembourgeois et d'autres services des Ministères Luxembourgeois se réfèrent aussi à nos articles !
CASES (LU)http://www.cases.lu
Pour ceux et celles qui ont la possibilité de lire des informations RSS, nous syndiquons aussi notre contenu par cette voie, dont voici les liens :
http://www.internetmonitor.lu/syndication.rss
http://www.internetmonitor.lu/atom.xml

Vous ne connaissez pas les fils RSS ? Pas de problèmes, veuillez cliquer le lien suivant et lire mon tutoriel à ce sujet : (Pas de connaissances techniques requises)
Blogs et RSS La syndication par fils RSS est le futur de la communication sur Internet !
Simple, rapide et efficace. Jamais le flux d'informations a pu passer si rapidement. Internet nous ouvre la voie de la communication !
Glossaire :
Malware : Mot regroupant les virus, vers, dialer et toutes autres bestioles informatiques.
Troyen (Trojaner/Trojan) : Programme malicieux cachant un deuxième programme malicieux.
Dialer : Programme générateur d'une communication surtaxée.
Anti-virus : Le système immunitaire de notre PC (obligatoire) !
Anti-Troyen : Programme protecteur et éradicateur de troyens.
Anti-Dialer : Programme protecteur et éradicateur de Dialer.
Anti-Spyware : Programme protecteur et éradicateur de Spyware (mouchards).
Polluposteur : Distributeur de courrier non sollicité (Spam)
Phishing : Détournement et usurpation d'identité d'un site Internet.
Firewall (pare-feu) : Le système anti-intrusion de notre PC (obligatoire) !
Newsletter : Lettre d'information envoyée par courrier électronique (email)

Liens :
Les 2 mondes :
Les 2 mondes http://www.webwizardbiz.com/tutorials/responsabilites/

Visual PC&Internet :
Visual PC&Internet
http://www.internetmonitor.lu/index.php?action=article&id_article=70793

Nétiquette :

Nétiquette http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html#intro

Chatiquette :
Chatiquette http://www.artetcraft.com/chat/netiquette.php
Malware :
Malware
http://www.homepages.lu/gust.mees/mausi/securite/malware/
Guide pratique de la sécurité :
Guide pratique de la sécurité
http://www.webwizardbiz.com/tutorials/guidesecurite/
Spyware :
Spyware
http://www.internetmonitor.lu/index.php?action=article&id_article=83305
Dialer :
Dialer http://www.webwizardbiz.com/tutorials/dialer/
Troyen :
Troyen
http://www.internetmonitor.lu/index.php?action=article&id_article=91039
Anti-Spyware installation :
Anti-Spyware installation
http://www.internetmonitor.lu/download/Spybot_S_D_Tutorial.pdf
Nos responsabilités dans Internet :
Nos responsabilités dans Internet
http://www.internetmonitor.lu/index.php?action=article&id_article=67346
E-book Security :
E-book Security
http://www.homepages.lu/gust.mees/pedago/ebook/index.html
Vigilance (Éditorial) :
Vigilance
Le nouveau monde, le monde virtuel :
Le nouveau monde, le monde virtuel
ZONELABS :
http://www.zonelabs.com

Comment savoir maintenant si notre PC est bien protégé, bien sécurisé ?

Vous allez certainement me dire maintenant, que j'ai bel et bien parlé, mais comment avoir confiance en mes conseils ?
Vous avez tout à fait raison de penser comme ça. Rien ne vaut un contrôle pratique pour s'assurer.
Pour ceci je vous propose deux (2) formules différentes :
1. Visitez mon tutoriel (Cours online gratuit) à l'adresse suivante et téléchargez-le (2 pages A4)

¨ Test online gratuit (en ligne) :

Online security check
2. Test des ports du PC, contrôler l'efficacité du *FIREWALL* (Pare-feu)

Test des ports du PC
Après les avoir téléchargé, suivez les instructions et vous serez beaucoup plus confiants après !
Mes autres sites Internet sur la sécurité PC&Internet :
Sécurité PC&InternetSécurité PC&Internet http://www.pcsecurite.org
Sécurité PC&InternetSécurité PC&Internet http://www.webwizardbiz.com/tutorials/security
Internet MonitorInternet Monitor http://www.internetmonitor.lu
MalwareMalwarehttp://www.homepages.lu/gust.mees/mausi/malware
Mes blogs sur la Sécurité PC&Internet :
http://www.internetmonitor.lu/pcsecurity
http://www.u-blog.net/pcsecurity
Syndication RSS et ATOM :
http://www.internetmonitor.lu/syndication.rss
http://www.internetmonitor.lu/atom.xml
Au cas où vous ne disposez pas de lecteur RSS (RSS-Reader), je peux vous conseiller Feed Reader, lequel vous pouvez télécharger (download) à l'adresse URL suivante :
Feed Reader http://www.feedreader.com
En plus vous trouverez mon tutoriel sur l'installation et l'utilisation de Feed Reader à l'adresse URL suivante :
Installation & utilisation Feed Readerhttp://www.internetmonitor.lu/download/feedreader_installation_et_utilisation.pdf

Récapitulatif :
Le PC et Internet ont créé un nouveau mass média, une base de données inépuisable, grandissante à chaque seconde. Ce mass média nous ouvre le monde de la communication et de l'information.
Pour tout ce qui est nouveau, il nous faut un certain temps pour nous habituer, nous familiariser, apprendre à nous servir de cette nouvelle technologie.
Toute nouvelle technologie requiert aussi un entretien technique et des consignes de sécurité !
Le PC et Internet n'y font pas exception !
Pour vous faciliter la tâche, j'ai créé un tutoriel pour la pratique quotidienne, le
Guide pratique de la sécurité, lequel vous trouverez à l'adresse URL suivante :
Guide pratique de la Sécurité

PC&Internethttp://www.webwizardbiz.com/tutorials/guidesecurite/
Tout ce qui a été expliqué dans ce tutoriel y est présent et expliqué comment faire la pratique
(Comment s'en servir) !
Essayez de suivre ce tutoriel à la lettre et votre vie réelle et virtuelle sera plus facile.
Happy and secure surfing !

Remarques
Pour créer ce tutoriel, il a fallu :
" 5 années d'expérience et d'apprentissage dur
" beaucoup de patience de ma compagne (un grand MERCI)
" de multiples révisions par des amis (MERCI Lex)
" beaucoup de courage et de persévérance
" +/- 300 magazines professionnels dans trois (3) langues (FR, DE, EN)
" *+- 20 livres et livrets ont été consultés sur la Sécurité PC&Internet en 3 langues
" Des centaines d'heures ont été nécessaires pour télécharger et essayer des programmes (logiciels) de sécurité et surtout à les comprendre, savoir les utiliser à fond pour pouvoir créer un tutoriel !
C'est pour les raisons mentionnées ci-dessus, que je vous demande, soyez gentils et honnête. Utilisez ce tutoriel à des fins privées et pour l'éducation, ceci gratuitement !
Pour une utilisation commerciale, même seulement des extraits, veuillez me contacter à l'adresse suivante : gust.mees@vo.lu
Si vous utilisez ce tutoriel pour l'éducation, il est bien évidemment GRATUIT, mais soyez gentils et veuillez m'en avertir et aussi placer un lien bien visible sur votre site Internet. Ceci me fera plaisir de voir que mon travail est respecté !
Cette compilation de la Sécurité PC&Internet est un résumé de +/- 300 pages A4, réduit à 9 pages A4. Ces 9 pages A4 ont été révisées +/- 85 fois avant de les publier !
Il a fallu quatre (4) mois de travail (+/- 2 hres/jour) pour la création de ce tutoriel (120x2=240 hres).
Et le prix de tout ceci = GRATUIT !
S.v.pl. Respectez le travail d'autrui ! Copier tout le monde sait le faire !
Si vous voulez vous vanter de votre travail, créez-le vous-même !
Au moins vous pouvez être fier de l'avoir fait vous-même et sans avoir peur d'être jugés un de ces jours par un tribunal pour atteinte à la propriété intellectuelle !
Peut-être il se cache de la stéganographie dans mon document ?????

Stéganographie
Copyright © by Gust MEES (LU) / Formateur pédagogique T.I.C.
T.I.C. = Technologies de l'Information et de la Communication

Tutoriaux (Cours gratuits) : C'est quoi un port ?

Gust MEES

Le mot *port* est au fait l'abréviation de *port de communication*. Au fait, le PC utilise 65535 de ces *ports*. Ces *ports* (portes) seront utilisés selon les besoins (commandes) du processeur.
Exemple : Si vous utilisez la commande *Imprimer*, le *port 139* servira pour cette action.

Chacun de ces *65 535 ports* a une signification exacte (normalisé) et ils sont pareils pour chaque PC !

Vous pouvez accéder à une liste complète de ces ports et de leur signification aux adresses URL suivantes :

http://www.iana.org/assignments/port-numbers

http://www.webwizardbiz.com/tutorials/firewalls/

L'assignation des ports est gérée par l'I.A.N.A. (Internet Assigned Numbers Authority) :

http://www.iana.org/

Ces 65535 ports peuvent être regroupés dans trois catégories :

1. Les ports bien connus 0 à 1023.
2. Les ports registrés de 1024 à 49151
3. Les ports dynamiques et ports privés de 49152 à 65535

Essayez de visualiser ces *ports* (portes) comme faisant partie d'une maison, une maison avec 65535 portes.

Au fait, un immeuble administratif avec 65535 collaborateurs dont chaque bureau (porte) est assigné un numéro de 1 à 65535.

Ces portes (ports) doivent bien entendu être protégés, sinon un intrus peut avoir accès pour voler et ou détruire du matériel y stocké !

Dans un immeuble ou une maison nous prenons recours à un système anti-intrusion (système d'alarme).

Pour le PC nous utilisons un *Firewall* (pare-feu). Le *Firewall* (pare-feu) protège nos *ports de communication*, il les surveille et nous avertit quand il y a une attente à notre sécurité ! Le *Firewall* peut être visualisé comme un portier contrôlant le trafic non désiré entrant et sortant.

Veuillez noter que le *Firewall* intégré de *WINDOWS XP* ne contrôle que le trafic entrant et pas le trafic sortant ! (19.12.2004.)

Il existe deux sortes de *Firewall* :

1. Desktop Firewall (logiciel / programme)
2. Hardware Firewall (Matériel physique ou intégré dans un ROUTER)

Pour les privés, les *Desktop Firewall* (logiciels / programmes) sont utilisés. Ces *Desktop Firewall* existent même en version gratuite (Freeware) dont notamment *ZONEALARM* du fabricant ZONELABS : http://www.zonelabs.com

Comment installer et configurer ZONEALARM ?

Vous trouverez à l'adresse URL suivante un très bon tutoriel :

http://www.cases.public.lu/publications/dossiers/firewall/Zonealarm/ZA3/index.html

Comment savoir maintenant si les ports de mon PC sont bien sécurisés ?

Il existe des services gratuits (pour usage non commercial) sur Internet où nous pouvons tester en ligne (online) la vulnérabilité des *ports* de notre PC, sans avoir besoin de connaissances techniques, accessible à tout le monde !

Un de ces services est *SECURITYMETRICS* http://www.securitymetrics.com

Ce service est en anglais.

Un autre bon service gratuit est *PORT-SCAN* http://www.port-scan.de

Ce service est en allemand.
Vous pouvez télécharger (download) le tutoriel avec screenshots comment faire ce test aux adresses suivantes :
En format WORD : En format WORD
En format PDF : En format PDF

Il n'y a pas de problèmes, seulement des solutions. Ensemble, nous trouverons la solution adéquate!

Mail : adcoet@pt.lu

Url : http://www.internetmonitor.lu