Internet Monitor Security News

EDITO

Bonjour chers internautes,

Dans cette édition vous trouverez une sélection de mes tutoriaux (cours gratuits online) sur la sécurité PC & Internet ainsi que des outils gratuits pour tester votre PC.

Le PC & Internet vous serons expliqués d'une manière transparente et non technique (Visual PC & Internet)!

Je vous souhaite bonne lecture et bon apprentissage.

Gust MEES / Formateur pédagogique TIC

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

Spyware (FR) : Earthlink publie son Top 10 des spywares

Gust MEES

Le fournisseur d'accès américain a dévoilé son classement des espiogiciels les plus répandus sur le Web. L'occasion de rappeler les dangers de ces logiciels intrusifs et les moyens de s'en prémunir.

Les spywares, ou espiogiciels, sont devenus depuis quelque temps l'une des principales nuisances pour les internautes. Ces programmes, installés à l'insu des utilisateurs généralement via des logiciels gratuits, ont pour mission de collecter sur les ordinateurs diverses données personnelles et de les transmettre à leurs auteurs, qui peuvent se révéler plus ou moins malintentionnés.

Tutoriaux (Cours gratuits) : Pourquoi cette tendance (trend) croissante des attaques virales ?

Gust MEES

À l'époque, les créateurs de virus étaient des vandales. Leur seul but était de se faire remarquer et de créer des virus destructifs.

De nos jours, les créateurs de *malware* (virus, vers, troyens, dialer, phishing scripts, etc.) poursuivent une toute autre politique et tactique. Les créateurs de ces *malware* ont découvert un marché lucratif (£, $, €) !

Sachez aussi que l'on appelle ces *criminels* désormais des *CRACKER* et non plus des *HACKER* !

L'expression *HACKER* est désormais utilisée pour des gens qui essayent de pénétrer dans un PC et ou réseau sans mauvaises intensions. Ils communiquent ces vulnérabilités alors aux fabricants des logiciels en question et avertissent les firmes où les réseaux ne sont pas assez sécurisés.

Marché lucratif, gagner de l'argent en créant des virus ?

Eh bien oui, même que des créateurs de *malware* n'agissent plus seuls, mais sont regroupés dans des clans bien organisés (une sorte de mafia informatique) !

Ils exploitent les PC non protégés (sans anti-virus et sans Firewall) qui se connectent à Internet. Ces Pc non sécurisés on les appelle désormais des *PC ZOMBIES* !

Cette mafia informatique fait un scan de la *Toile* (Internet) pour trouver ces *PC ZOMBIES* (PC non protégés), leur refile un *Troyen* (contenant un Keylogger et un Backdoor) et les téléguide (contrôle) ensuite à l'insu de leurs propriétaires !

Ceci est seulement la première partie de leur stratégie. Une fois ces *PC ZOMBIES* infectés par ces *Troyens*, ils les connectent ensemble comme dans un vrai réseau et les utilisent comme une plate-forme géante pour envoyer du courrier non sollicité (SPAM) dans le meilleur des cas !

Sinon, les PC infectés par cette sorte de *Troyens* sont *violés* pour stocker des sites pornographiques sur leurs disque dur à leurs insu (sans qu'ils s'en aperçoivent).
Bien entendu, l'accès à ces sites pornographiques (hébergés sur votre PC) est payant !

Ces *PC ZOMBIES* seront connectés ensemble, on appelle cette pratique un *botnet* et ils forment un réseau d'échange de fichiers, similaire au *P2P* (peer to peer). Presque impossible de détecter les vrais malfaiteurs. Et pourtant, parfois des réseaux criminels sont détectés ; voir l'article suivant :

Démantèlement d'un réseau de 10.000 PC zombies

Ces réseaux criminels sont même loués et offrent un revenu lucratif pour leurs créateurs (€, $, £) !

Voir l'article suivant :

Votre PC est-il un «zombie» à louer ?

Dans le pire des cas ces *PC ZOMBIES* sont utilisés pour faire une attaque *DOS* contre un site Internet bien défini, comme ceci s'est déjà passé contre le site Internet de SCO (et avec succès !) dont voici

l'article :

Le virus MyDoom réussit son attaque contre le site SCO

Un autre truc consiste à utiliser une faille majeure de l'Internet Explorer (IE).
La fonction *Active X* dans l'Internet Explorer est très dangereuse. Elle permet d'exécuter du *scripting* (code de programmation) !

Votre PC peut être dévié envers un site Internet que vous n'ayez choisi. On appelle ceci du *BROWSER HIGHJACKING*.

Afin d'éviter cette action de *HIGHJACKING*, il faudra jouer un peu sur les réglages de sécurité de l'Internet Explorer.

Vous pouvez télécharger (download) le tutoriel complet aux adresses suivantes :
Version WORD (279,5 KB)
Version PDF (858,2 KB)

Tutoriaux (Cours gratuits) : Automatiser l'anti-virus *Norton Internet Security* et *Norton anti-virus*

Gust MEES

Avec le logiciel *Norton anti-virus* et *Norton Internet Security* nous avons un outil très puissant à notre disposition. Même que cet outil précieux et inévitable est capable d'automatiser certaines fonctions.

Automatiser, comment et quoi ?

Ce logiciel (programme) a une fonction que l'on pourrait appeler *Gérance des tâches* (Task manager). Avec cette fonction il nous est possible d'automatiser le scan de notre disque dur.

En termes claires : Notre PC est sous tension (allumé) et nous voulons que l'anti-virus scrute (scan) notre disque dur sur des infections virales à un moment donné, sans notre intervention manuelle.

Pas de problèmes, ceci est réalisable. Dans mon tutoriel (cours gratuit en ligne), vous trouverez les explications comment faire les réglages nécessaires.

Le tutoriel ne comporte que deux (2) pages A4 et le temps de réalisation ne dépasse pas les cinq (5) minutes !

Qu'attendez-vous pour le télécharger et vous faciliter la vie ? À vos claviers, prêt et tapez l'adresse suivante : Page 1/2... et ...Page 2/2

Tutoriaux (Cours gratuits) : 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

Tutoriaux (Cours gratuits) : Attaque réelle de *Troyens*

Gust MEES

Case study :

Comment réagir lors d'une attaque de *Troyens* sur mon PC ? Est-ce que vous ne vous êtes pas déjà posés cette question ?

Pour les PC protégés d'un anti-virus et Firewall, pas de problèmes. Je vous montrerais maintenant comment faire en me basant sur un exemple pratique.

Pour ceux qui n'ont pas installé de logiciels de protection, ils ne sont apercevront même pas de ces attaques et les Troyens s'installeront sur leur PC !

Leur PC deviendra un *PC ZOMBIE* !

Je me suis payé le luxe d'aller chercher des *Troyens* sur Internet pour écrire ce tutoriel. Eh bien, croyez moi, c'est très facile d'en trouver et beaucoup plus facile que je m'imaginais ! (Pas plus de cinq minutes !)

Il suffit de scruter la *Toile* (Internet) en visitant des sites à caractère *xxx* et le fait simple de cliquer sur un lien et ou bien de visiter un site *xxx* quelconque pour attraper ces bestioles informatiques.

Quand vous visitez des sites d'échange de fichiers P2P, c'est pareil. Une étude a démontré que +/- 45% des fichiers téléchargés étaient contaminés.

Pour voir le tutoriel, veuillez cliquer le lien suivant pour le télécharger en format PDF (1,9 Mb). Un peu lourd (1,9 Mb) mais cela vaut la peine de le suivre avec pleins de *screenshots* et explications non techniques (pédagogique) !
Attaque réelle de *Troyens*
http://www.internetmonitor.lu/download/(Microsoft_Word_-_Case_study-Attaque_r_351elle_14.11.2004..doc).pdf
Copyright (C) by Gust MEES (LU)

Security News (FR) : SecureConnect: le savoir-faire des P&T au service de vos réseaux d'entreprise !

Gust MEES

L'accès fiable à l'Internet

SecureConnect Web Access sécurise votre accès Internet et constitue un rempart efficace contre les attaques subies par votre réseau et les tentatives d'accès non autorisés.

Vos avantages:
• un système de gestion du firewall basé sur une interface web simple qui vous permet de créer et de gérer votre propre politique de sécurité

• une protection de vos applications et boîtes e-mails grâce à un service de détection de virus

• la garantie d'un anti-virus mis à jour automatiquement par les P&T

• une solution simple qui ne nécessite aucun expert en sécurité ou en réseau au sein de votre entreprise.

La communication sécurisée entre vos collaborateurs et votre réseau d'entreprise

Avec SecureConnect Remote Access, chacun de vos collaborateurs mobiles (télétravailleurs, techniciens, etc.) bénéficie d'un accès direct et sécurisé aux données dont il a besoin.

Vos avantages:

• une connexion Internet sécurisée

• un accès sécurisé aux données d'entreprise avec la possibilité d'un partage sécurisé de celle-ci

• une équipe d'experts P&T se charge pour vous de la configuration et de la gestion du service.

L'intranet sécurisé contre tout accès non autorisé

SecureConnect Network Access permet une communication optimale entre les réseaux informatiques locaux de vos sites distants et celui de votre site central grâce à une vitesse d'échange de données élevée et totalement sécurisée.

Vos avantages:

• un véritable réseau privé (VPN-Virtual Private Network) entre votre site central et vos succursales

• l'installation, la gestion et la maintenance du service assurées par une équipe d'experts P&T

• une redevance mensuelle fixe totalement abordable.

Pour votre sécurité, faites confiance au P&T!
Renseignements supplémentaires au téléphone gratuit 12 422.

Entreprise des P&T
EPT

Article fourni et autorisé pour publication par le Service de Presse des P&T

Éditorial : Fils RSS (RSS Feeds) et BLOG's (Web Logs)

Gust MEES

À la mode sont actuellement la syndication de contenu (le contenu de votre site Internet peut être employé sur d'autres sites Internet) et les BLOG's.

Le monde virtuel (Internet) grandit et presque chaque jour il y a des nouvelles possibilités. L'outil communicatif (Internet) nous élargit une fois de plus la bande passante des possibilités pour nous exprimer et de recevoir des informations gratuites !

Pour tous ceux qui aiment s'informer et recevoir toujours des nouvelles fraîches (sport, monde, IT, TIC, etc.) les fils RSS (RSS FEEDS) sont de premier choix et très facile à utiliser.
Il suffit d'installer un logiciel (programme) sur notre PC pour lire les fils RSS. Un programme (logiciel) gratuit et très facile à utiliser est « Feed Reader » que vous pouvez télécharger à l'adresse suivante : Feed Reader

Figure 1 : Mon fils RSS de http://www.internetmonitor.lu/syndication.rss
Mais sachez aussi que quelques navigateurs (Browser) ont un lecteur RSS intégré, tels que OPERA et FIREFOX.

Une fois le logiciel (programme) installé, il suffit d'aller faire son choix dans les offres (catalogues) de fils RSS et les intégrer dans le lecteur de fils RSS en employant le copier et coller (drag & drop).

C'est tout ce qu'il faut faire. Votre lecteur de fils RSS est en veille et dès parution (changement) de contenu de fils RSS, il vous avertira automatiquement et vous montrera les nouvelles sur le bureau de votre PC (seulement avec connexion Internet).

Recevoir les dernières nouvelles sans se soucier et sans se fatiguer et GRATUIT en plus !

Ayant parlé des avantages de recevoir quelque chose de gratuit, Internet nous donne aussi la possibilité de pouvoir donner quelque chose ; c.à.d. de communiquer.

Avec les blogs, abréviation de Web Log, nous pouvons écrire des petits commentaires et les publier sur Internet, sans avoir de

connaissances de programmation.

Soit que nous voulons seulement exprimer notre mécontentement sur un sujet qui nous touche, faire un journal intime, exprimer notre mal d'amour pour les jeunes et celles (et ceux) qui sont resté(e)s jeunes ou seulement écrire quelque chose, parce que nous éprouvons un besoin de communiquer.

Avec les blogs (web logs) nous avons la possibilité de nous exprimer, la liberté de parler (écrire) !

Les blogs reflètent les pensées du monde entier.

Les blogs font actuellement la fureur sur Internet et ils sont en train d'envahir le monde virtuel (Internet). La liberté de pouvoir s'exprimer, où est-ce que cela existe-t-il encore ? Sur Internet, bien sûr.

Et en plus les blogs sont gratuits et pas besoin d'avoir des connaissances de programmation !

Les blogs sont accessibles à tout le monde !

Des fournisseurs de blogs intéressants sont :

BLOGGER : BLOGGER

U-BLOG : U-BLOG

WMAKER : WMAKER

Faites-en un petit tour sur Internet, visitez les sites mentionnés ci-dessus, consultez quelques blogs pour vous faire une idée et décidez vous-même si oui ou non, cela vous tentera de *blogger*.

À vos claviers, prêt, à l'attaque. La liberté d'expression à vos mains !

Catalogues RSS :

http://www.2rss.com : http://www.2rr.com

http://www.lamoooche.com : http://www.lamoooche.com

http://www.rssscout.de : http://www.rssscout.de

http://www.rss-verzeichnis.de : http://www.rss-verzeichnis.de

Quelques blogs de notre *Internet Stuff* :

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

http://www.internetmonitor.lu/femmesdunord : http://www.internetmonitor.lu/femmesdunord

http://www.internetmonitor.lu/grosbusch : http://www.internetmonitor.lu/grosbusch

En bref : Avec ces deux nouvelles possibilités, Internet devient encore plus communicatif et intéressant.

Le savoir du monde entier à notre portée (24h/24h) et la liberté de s'exprimer!

Gust MEES

Security News (DE) : INSAFE: Start eines europaweiten Netzwerks zur sicheren Nutzung des Internet

Gust MEES

Am 18. und 19. November wird INSAFE, ein europäisches Netzwerk zur Bewusstseinssteigerung, das sich mit den Herausforderungen nationaler, europäischer und internationaler Agenden beschäftigt, in Prag gegründet. Der Aufbau des Netzwerks ist ein wichtiger Schritt im Aktionsplan für sichere Nutzung des Internet der Europäischen Kommission (SIAP).

Die Koordination der unzähligen, facettenreichen Initiativen, die

täglich rund um den Globus stattfinden, ist auf die nationalen Bewusstseinskampagnen zur sicheren Nutzung des Internets abgestimmt, welche die Aktionen auf nationaler Ebene koordinieren. INSAFE zielt darauf ab, den Austausch und das Sammeln von Expertisen und Ressourcen zwischen Informationsnetzwerken und anderen wichtigen Akteuren in Europa und weltweit, zu optimieren.

Es wird vom European Schoolnet in Partnerschaften mit der Cyberspace Research Unit der Universität von Central Lancashire (UK) und dem Norwegian Board of Film Classification durchgeführt. Die Initiative wird vom Europarat unterstützt.

Das Eröffnungstreffen des Netzwerks findet im Rahmen der jährlichen EMINENT Konferenz des European Schoolnet, die führende Experten und nationale politische Entscheidungsträger miteinander in Kontakt bringt, statt. Die Präsentation von INSAFE bei einem derart wichtigen Bildungstreffen macht die Aktion zur sicheren Nutzung des Internet im gesamten Bildungsbereich bekannt.

Angesichts der momentanen Auswirkungen des Internets auf die Gesellschaft erscheint es unerlässlich, Internetfertigkeiten sowie das Thema der Internetsicherheit im Schulbereich zu thematisieren.

Heterogene Natur der Bewusstseinssteigerung
Internetsicherheit geht weit über die Grenzen des Bildungsbereiches hinaus. Dies reflektiert die heterogene Natur der 14 nationalen Netzwerke, aus denen die INSAFE Gemeinschaft besteht. Im Moment nehmen Österreich, Belgien, Dänemark, Finnland, Deutschland, Griechenland, Island, Irland, Italien, die Niederlande, Norwegen, Portugal, Spanien und das Vereinigte Königreich an der Aktion teil. Weitere Akteure werden in den nächsten Monaten dazustoßen. Vier wesentliche Aktivitätsbereiche, vertreten von Partnern verschiedenster Bereiche, sind am Gesamtnetzwerk beteiligt:

Beratende und regelnde Körperschaften
Öffentliche Abteilungen und Institutionen
Verbraucherschutzagenturen
Humanitäre Organisationen
Bildungsindustrie
Abgrenzung der Herausforderung

Grundsätzlich sind bewusstseinsfördernde Aktionen mit einer dreifachen Herausforderung konfrontiert:

die Bürger zu schulen, moderne Informations- und Kommunikationswerkzeuge effektiv einzusetzen

sie vor den physischen und ethischen Gefahren des Internet zu schützen
ihre fundamentalen Menschenrechte der Privatsphäre, Sicherheit und des Eigentums (z.B. Autorenrechte) zu schützen

Wesentliches Ziel von INSAFE ist die Koordination und Stärkung jener Aktionen, die von nationalen Netzwerken durchgeführt wurden und ihre Präsentation nach außen zu verbessern.

Dank seiner langen Erfahrung im Bereich der Netzwerkkoordination bietet das European Schoolnet einen organisatorischen Rahmen und umfangreiche Werkzeuge, um die Nachhaltigkeit des Netzwerks zu gewährleisten. Fortschritte werden von einer Lenkungsgruppe bestehend aus nationalen Netzwerken und dem Koordinationsteam kontrolliert.

Ziel ist es, nicht nur die Arbeit nationaler Netzwerke zur sicheren Nutzung des Internet, sondern auch jene von Einzelpersonen, Organisationen und Agenturen in diesem Bereich zu unterstützen und zu fördern.

Geplante Aktivitäten umfassen:

Die Entwicklung einer dreisprachigen europäischen Schnittstelle für Informationen, Werkzeuge und Ressourcen

Einen regelmäßigen Newsletter mit aktuellen Informationen über wichtige Themenbereiche
Eine europaweite Begutachtung entstehender Risiken und innovativer Schutzmechanismen
Trainingsworkshops zu diversen Facetten der Bewusstseinssteigerung, z. B. Auswirkungsanalyse, Veranstaltungsplanung, Optimierung der Medienreichweite.

Den Entwurf eines Onlinebaukastens bestehend aus "guten Praxisbeispielen", die in verschiedensten kulturellen Umgebungen eingesetzt werden können
Die Verteilung von Umfrageblättern für Verbraucher und ein sechsmonatiger Bericht, um die Qualität und Verbreitung zu optimieren

Mechanismen zum verbesserten Informationsaustausch zwischen den einzelnen Teilnehmern.

Zurück in die Zukunft

Das Eröffnungstreffen in Prag baut auf jenen Ressourcen auf, die in früheren SIAP Aktionen erarbeitet wurden, und bietet einen Rahmen für schlüssige, koordinierte und umfangreiche Strategien zur sicheren Nutzung des Internet in Europa. In einer Zeit, in der Bandbreiten größer werden und sich mobile Technologien einander annähern, kann die Herausforderung für die Sichere Internetnutzung nur wachsen. INSAFE strebt danach, Erfahrungsreichtum dazu zu nutzen, negative Einflüsse abzuwehren und das Internet als das zu fördern, was es ist: eine wertvolle Ressourcen für die Bildung, Unterhaltung und die vielen kleinen banalen Aufgaben des täglichen Lebens.

Für weitere Informationen kontaktieren Sie bitte: janice.richardson@eun.org

Für ein Abonnement der INSAFE Mailingliste wenden Sie sich bitte an:camilla.sand@eun.org

Quelle des Artikels: European Schoolnet
http://www.eun.org/eun.org2/eun/en/About_eschoolnet/content.cfm?lang=de&ov=33951&id_area=101

Security News (FR) : INSAFE : Lancement d'un réseau européen pour un Internet plus sûr

Gust MEES

Le lancement de INSAFE a eu lieu à Prague les 18 et 19 novembre. Ce réseau européen de sensibilisation à la sécurité en ligne a pour objectif de relever un défi qui prend de plus en plus d'importance aux niveaux nationaux, européen et international. La mise en place de ce réseau constitue une avancée considérable dans le Plan d'Action pour un Internet plus sûr de la Commission européenne.

INSAFE vise à optimiser la valeur ajoutée européenne par le biais de l'échange et de la collecte d'expériences et de ressources entre organismes et autres acteurs clés d'Europe et du reste du monde.

Ce réseau est géré par European Schoolnet en partenariat avec la Cyberspace Research Unit de l'Universite de Central Lancashire (Royaume Uni) et le Norwegian Board of Film Classification. Cette initiative reçoit le soutien du Conseil de l'Europe.

Le lancement du réseau a eu lieu dans le cadre de la conférence annuelle EMINENT organisée par European Schoolnet, laquelle réunit experts de pointe et décideurs nationaux dans le domaine de l'éducation. La planification de cet événement dans un contexte éducatif plus général élargit le champ de visibilité des actions pour un Internet plus sûr menées dans l'éducation.

Etant donné l'impact actuel d'Internet sur notre société, il apparaît crucial d'intégrer l'apprentissage de compétences en Internet au concept plus général d'apprentissage et de mettre la sécurité en ligne à l'ordre du jour une fois pour toutes.

Nature hétérogène de la sensibilisation à Internet.

Toutefois, la sécurité sur Internet dépasse les frontières de l'éducation. Cela se reflète dans la nature hétérogène des 14 organismes nationaux de sensibilisation à Internet qui constituent pour l'instant la communauté INSAFE. L'Allemagne, l'Autriche, la Belgique, le Danemark, l'Espagne, la Finlande, la Grèce, l'Islande, l'Italie, la Norvège, les Pays-Bas, le Portugal et le Royaume Uni sont actuellement membres du réseau. D'autres organismes viendront officiellement allonger la liste dans les mois à venir. Quatre secteurs d'activités importants sont représentés, certains organismes combinent des partenaires dans plusieurs domaines :

Organismes de conseil, de consultation et de régulation
Départements et institutions publiques
Agences de protection des consommateurs
Organisations humanitaires
Industries de l'éducation
Définir le défi à relever

Les sensibilisateurs doivent faire face à un triple défi :

permettre aux citoyens d'utiliser efficacement les TIC modernes et de tirer pleinement profit de tout ce qu'elles ont à offrir

protéger ces citoyens contre les dangers que présente Internet, qu'ils soient d'ordres physique, social ou éthique

sauvegarder leurs droits fondamentaux à la vie privée, à la sécurité et au droit de propriété (ex. : droits d'auteur)

Le principal objectif de INSAFE est de coordonner et de renforcer les

actions entreprises par les organismes nationaux et d'en améliorer la visibilité. Grâce à sa longue expérience dans le domaine de la coordination de réseaux, European Schoolnet offre un cadre organisationnel et un ensemble exhaustif d'outils qui permettront d'assurer la durabilité du réseau.

Les progrès seront aiguillés par un comité directionnel qui combine les expériences des organismes nationaux et l'équipe de coordination du réseau. L'objectif est d'encourager et de promouvoir le travail des organismes nationaux de sensibilisation à un Internet plus sûr d'une part, et celui de tous les individus, organisations et agences actifs dans le domaine d'autre part. Parmi les activités prévues figurent :

Le développement d'un portail européen disponible en trois langues offrant informations, outils et ressources

Un bulletin d'informations régulier offrant des mises à jour sur des questions importantes
Un contrôle au niveau européen des risques émergeants et des mesures de protection innovantes

Des ateliers de formation sur les différentes facettes de la sensibilisation. Ex. : contrôle des impacts, planification d'événements, optimisation de l'impact des médias

La création d'un kit en ligne de « bonnes pratiques » transposable dans différents environnements culturels

La diffusion d'études abordant la satisfaction des utilisateurs et de rapports de progrès tous les six mois pour optimiser qualité et portée

Un mécanisme d'échange entre les organismes de sensibilisation nationaux pour faciliter le partage de connaissances.

Retour vers le futur

La réunion de Prague sera basée sur les ressources développées ultérieurement dans le cadre d'actions menées pour le Plan d'action pour un Internet plus sûr. Elle offrira un cadre pour des stratégies européennes cohérentes, concertées et complètes en matière d'Internet plus sûr. Plus les technologies mobiles et le haut-débit convergent, plus le défi prend de l'importance. INSAFE aspire à utiliser la riche expérience de sa communauté pour combattre les influences négatives et promouvoir Internet pour ce qu'il est, à savoir une ressource de valeur pour l'éducation, un divertissement et un outil facilitant les nombreuses tâches banales du quotidien.

Source de l'article : European Schoolnet
http://www.eun.org/eun.org2/eun/fr/About_eschoolnet/content.cfm?ov=33951&lang=fr

Tutoriaux (Cours gratuits) : Testez votre logiciel (programme) anti-virus

Gust MEES

**
**

Est-ce que vous faites part des personnes qui ne croient ce qu'ils voient ? Alors exposez votre logiciel (programme) anti-virus à une attaque virale réelle, inoffensive, mais efficace.

Pour faire ceci, je vous invite à suivre mon tutoriel. Dans ce test vous injecterez un virus inoffensif dans votre système (PC), soit par envoi e-mail (courrier électronique) et ou en ouvrant un fichier.

Testez votre logiciel anti-virus

En tout cas, votre système de protection, votre logiciel (programme) anti-virus devrait reconnaître ce virus simple et inoffensif !

Ce test vous donnera la satisfaction du bon fonctionnement de votre logiciel (programme) anti-virus !

Dans ce tutoriel (workshop) vous pouvez aussi suivre étape par étape, comment vous débarrasser du virus mis en quarantaine par votre logiciel (programme) anti-virus.

Dans notre exemple se sera *Norton Internet Security*.

Nous ouvrons notre navigateur (Browser), dans notre cas, Internet Explorer 6 et nous entrons l'adresse URL dans le champ de texte : EICAR
http://www.eicar.org/anti_virus_test_file.htm
Pour continuer notre tutoriel, veuillez cliquer le lien suivant :
à télécharger (PDF / 586 Kb) : Testez votre logiciel anti-virus

Security News (FR) : Lancement du portail de sécurité CASES Luxembourg

Gust MEES

Lancement du portail de sécurité CASES au Luxembourg.
CASES (Cyberworld Awareness Security Enhancement Structure) est le portail de la sécurité de l'Information au Luxembourg.
CASES est une initiative de plusieurs pays européens, qui prévoit la mise en place d'un réseau opérant dans le domaine de la sensibilisation et de la prévention visant l'établissement d'une culture de sécurité commune.

Actuellement le réseau CASES est composé des pays suivants :
Luxembourg
Belgique
Grèce
Grande-Bretagne
Hollande
Italie
Slovénie et
la Suisse.
Pour accéder au site Internet de CASES, veuillez cliquer ici.
http://www.cases.lu

Tutoriaux (Cours gratuits) : Troyens, Trojans, Chevaux de Troie

Gust MEES

C'est quoi un *Troyen* ?

L'expression *Troyen*, *Trojan horse* , *Trojan* ou encore *Cheval de Troie*, est dérivée de la mythologie grecque.

Comme les grecs cachaient des soldats dans le ventre d'un cheval en bois lors de la guerre contre Troie, cette malware (Troyen) en fait pareil.

Le *Troyen* est un programme malicieux qui en cache un autre. Le programme caché est en principe un *Keylogger*.

Le *Keylogger* lui-même est un programme qui enregistre toutes les frappes de clavier et qui ensuite envoie toutes ces données enregistrées à son programmeur vers l'intermédiaire du programme principal qui l'héberge.

Le programme principal, qui héberge le *Keylogger*, s'intègre dans la base des registres à votre insu (sans que vous vous en apercevez) et prépare l'envoi vers son programmeur.

Il ouvre certains ports de communication vers l'extérieur. Ces ports une fois ouverts, son programmeur peut avoir accès à votre PC et le téléguider !

Cette sorte de *Troyen* est appelé aussi un programme *backdoor*.

Téléguider mon PC ?

Eh bien oui, c'est possible !

Le premier programme malicieux (principal) ouvre les ports de communication (à voir comme une maison avec les portes principales grandement ouvertes).

Lire aussi : Firewalls

Le deuxième programme malicieux, le *Keylogger* a copié toutes vos frappes de clavier, tels que vos mots de passe, numéros de carte de crédit, vos données d'accès à vos comptes de sites Internet etc.
Toutes ces données seront envoyées et connues par le programmeur de ce code malicieux.

Ces deux combinaisons dans un programme malicieux sont très dangereuses.

Comment attraper un *Troyen* ?

On peut attraper un *Troyen* :

1. En ouvrant un courrier électronique (e-mail) d'une personne inconnue. En principe ils sont cachés dans les pièces jointes (attachments).
2. Par l'intermédiaire des portails P2P, les portails d'échange de fichiers.

Kazaa : 45% des fichiers exécutables seraient infectés

Si vous téléchargez des logiciels ou des jeux vidéo de Kazaa, vous pourriez obtenir plus que vous n'en demandiez puisque près de la moitié des fichiers exécutables seraient infectés par des virus, vers informatiques ou chevaux de Troie.

Lien de cet article :

Kazaa

Quel but poursuivent les programmeurs de ces codes malicieux ?

Le but en est bien évidemment commercial.

Commercial, comment ?

Si votre PC peut être téléguidé comme énoncé ci-dessus, cela veut dire que le programmeur du code malicieux (Troyen) est en mesure de faire avec votre PC ce qu'il veut !
Surpris ? Eh bien oui, Votre PC peut être téléguidé et vous ne vous en apercevrez même pas !

Dès connexion à Internet, sans protections de sécurité sur votre PC, votre PC est exposé à des intrusions. À voir comme un maison sans système d'alarme et ayant toutes les portes et fenêtres grandement ouvertes ! Un intrus (cambrioleur) peut entrer et sortir à votre insu (sans que vous vous en apercevrez) !

Mais revenons maintenant au but commercial. Ces programmeurs travaillent dans des groupes bien organisés (sorte de mafia informatique) et ils louent votre PC à des polluposteurs (envoyeurs de Spam) ! Et ils gagnent bien leur pain (£, $, €) avec cette méthode.
Là vous êtes certainement encore beaucoup plus étonnés, n'est-ce pas ?

Mais c'est la réalité, malheureusement !

Votre PC sera transformé en *PC ZOMBIE*, un PC téléguidé et employé pour des actions illégales !

Pour voir à quel point ces actions illégales sont déjà présentes, veuillez cliquer les liens suivants :

PC ZOMBIES

PC ZOMBIES 2

Une autre variante de se servir de votre PC, consiste à déposer du contenu illégal sur votre disque dur (Hard Disk) et dès que vous êtes connectés à Internet, de faire profiter les autres internautes à faire des téléchargements illégaux de ces contenus. En principe il s'agit de contenu pornographique et ou pédophile !

Vous hébergerez du contenu illégal sur votre disque dur sans le savoir !

Imaginez vous votre maison avec toutes les portes et fenêtres ouvertes et que des masses de personnes inconnues circulent. Du va et vient sans votre contrôle ! Est-ce que ce serait normal pour vous ? Sincèrement, je ne crois pas.

Mais l'exemple de réflexion ci-dessus vous montre bel et bien ce qui se passe *visiblement* quand votre PC n'est pas équipé de Firewall (pare-feu) !

Dès connexion à Internet, votre PC est visible par des millions d'internautes sur Internet et les brigands n'attendent que ça pour vous prendre comme prochaine victime !

En installant un Firewall (pare-feu) votre PC devient invisible sur Internet et les risques seront réduits à un minimum.

Comment tester si mon PC est bien protégé ?

Faites en un test online, ceci gratuit à l'adresse suivante :

Portscan GRATUIT

Maintenant que nous savons ce que c'est un *Troyen* et quels dégâts qu'il peut provoquer, nous nous poserons certainement la question :

Comment nous protéger ?

1. D'abord il faut installer un Firewall (pare-feu).Un portier qui contrôle le trafic entrant et sortant.
2. Comme protection supplémentaire, qui nous protège contre les *Troyens* et qui éradique aussi les *Troyens* installés sur notre PC, il nous faut installer un logiciel (programme) anti-troyen.

Le Firewall (pare-feu) nous protège contre les données entrantes et sortantes non désirées. C'est-à-dire : si jamais il y aurait un *Troyen* installé sur notre PC, il bloquerait sa connexion vers l'extérieur, mais le *Troyen* serait toujours résident sur notre PC !

Pour nous protéger contre les *Troyens* et surtout les éradiquer de notre PC, le cas échéant, il nous faut installer un logiciel (programme) anti-troyen.

Je vous conseille a2 de Emsisoft que vous pouvez télécharger gratuitement à l'adresse URL suivante :
Emsisoft (a2)

C'est un logiciel anti-malware (anti-troyen, anti-dialer etc,.) et multi langues qui nous protège et qui éradique aussi les malware.

Explication détaillée et technique d'un *Troyen* de a2.

Un tutoriel concernant le téléchargement et l'utilisation de *a squared (a2)* peut être trouvé à l'adresse suivante :

Tutorial a2

Je vous conseille aussi de lire mon tutoriel suivant :

Visual PC & Internet
Copyright (C) by Gust MEES (LU)

Figure 1 : L'Anti-virus NORTON INTERNET SECURITY et A2 scannent le PC

Glossaire :

Troyen, Trojan, Trojan horse : Cheval de Troie

Backdoor : Cheval de Troie réputé et très dangereux
Port : Port de communication du PC. Il en existent 65535
P2P ou *Peer to Peer* : Échange de fichiers
Kazaa, Emule, Edonkey : Portail d'échange de fichiers
PC Zombie : PC téléguidé et non sécurisé
Firewall (pare-feu) : Protection des données. Portier électronique.
Malware : Toute sorte de code malicieux (ver, virus, troyen, etc.)

Tutoriaux (Cours gratuits) : Comment contrôler notre PC s'il est sécurisé ou vulnérable

Gust MEES

Est-ce que mon PC est vraiment sécurisé, comment en être sûr? Est-ce que vous ne vous en êtes pas posés déjà cette question?

Sur vos questions il y a une réponse et en plus c'est GRATUIT et très simple à utiliser.

Veuillez télécharger (download) mon tutoriel à l'adresse suivante :
Free online PC Security Scan&Check
Le fichier en format PDF ne pèse que 218 Kb et le tutoriel est créé en format *workshop* pourque vous puissiez le suivre pas à pas.
Imprimez ce document (2 pages A4) et suivez les instructions.
Après avoir fait le test online, vous auriez la certitude exacte du status de sécurité de votre PC.
Copyright by Gust MEES (LU)

Tutoriaux (Cours gratuits) : Les dangers sur Internet en chiffres

Gust MEES

Internet nous réserve pas mal de surprises. Le monde virtuel (Internet) est plein de dangers lesquels il faut essayer de contourner et essayer aussi de les comprendre.

Au fait, ces dangers ne sont rien de nouveau, il faut tout juste nous les rappeler, car se sont exactement les mêmes dangers que dans le monde réel, notre vie quotidienne. Seule différence est, que nous ne sommes pas encore habitués à ce nouveau monde, car nous sommes des nouveaux-nés dans le cyber world (Internet) et comme des nouveaux-nés dans le monde réel (notre monde) nous devons suivre un apprentissage, un apprentissage à la vie virtuelle !

Juste pour vous rappeler les dangers dans le monde réel (notre monde) et puis les comparer avec les dangers dans le monde virtuel, voici un petit tableau comparatif :

Monde virtuel (Internet)
Remède
Monde réel (notre monde)
Remède

Virus, vers
Anti virus
Grippe, Virus
vaccin

Nouveaux virus
Signatures de virus (updates)
Nouveaux virus
Nouveau sérum

Spam (courrier non sollicité)
Filtre et programme anti-spam
Publicité dans les boîtes aux lettres
Jeter à la poubelle

Hacker, troyen etc.
Firewall (pare-feu)
Cambrioleurs
Systèmes d'alarme

Internet est le miroir de notre société ! Nous voyons nous même le comportement de tout le monde !

Comme vous pouvez le constater maintenant en regardant le tableau comparatif, la vie virtuelle n'est pas si différente, à voir même pareille que la vie réelle !

Au fait, comme Internet est créé et vie par l'intermédiaire de l'être humain, Internet représente les caractéristiques de notre monde. Logique, non ? Nous nous copions dans le monde virtuel avec nos habitudes positives et négatives !

Lire aussi mes articles : Nos responsabilités dans le monde virtuel

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

Visual PC & Internet

http://www.internetmonitor.lu/index.php?action=article&id_article=67449&id_rubrique=8949

Internet c'est nous, la communauté ! Voilà, ayant expliqué un peu le fonctionnement d'Internet, passons-en maintenant aux dangers d'Internet.

Les dangers d'Internet en chiffres :

Les *malware* (vers, virus, espionnage, phishing etc.) sont présents partout et même il y a une hausse de distribution de ces bestioles informatiques, du à la non connaissance (ignorance) des internautes (nous) !

Voici les chiffres :
• Actuellement il y a 100.000 virus informatiques
• 15.000 nouveaux virus ont été créés cette année
• 18 millions de PC's ont été infectés par le virus SASSER
• 250.000 atteintes de phishing/mois ont été enregistrées
• 1,2 milliards € de pertes ont été constatées aux États Unis par GARTNER par le biais de vol de numéros de cartes de crédit et de mots de passe.
• 50 nouveaux patches (rustines) de MICROSOFT sont publiés par année, sans compter les publications de MACTINTOSH et LINUX.
• 85 % du courrier électronique mondial se compose de *Spam*, de courrier non sollicité !

C'est cela les enjeux d'Internet. Et vous croyez toujours qu'il faut attendre que quelqu'un d'autre nous donne la solution ? Eh bien non, pas si vite. Franchement, pour la liberté il faut combattre nous même, comme dans le monde réel. Pour Internet c'est pareil.

Moi combattre ? Comment et pourquoi ?

En ce qui concerne la sécurité PC & Internet, nous pouvons tous faire quelque chose. Déjà en installant un anti virus et un firewall (pare-feu), nous réduisons la propagation des malware sur Internet et sur les PC. Si tout le monde aurait installé un anti virus et un firewall et en plus fait régulièrement les updates (MAJ) de chez MICROSOFT, le monde virtuel (Internet) serait plus au moins sécurisé.

En ce qui concerne le *Spam*, nous pouvons le combattre partiellement en sacrifiant un peu de notre temps.
Par exemple pouvons nous regarder qui nous envoie le *Spam* et l'identifier. Si l'expéditeur n'a pas falsifié son adresse e-mail, nous pouvons retrouver son FAI (ISP) et faire une plainte contre cette

personne. Cette personne perdra son compte Internet auprès de son ISP (FAI) et devra trouver un autre pour être raccordé à nouveau à la Toile (Internet). Une fois perdu son compte Internet chez un FAI (ISP), le nom de cette personne sera inscrite dans une liste noir et sera surveillée à ne plus faire d'abus de son compte !

Un de plus en moins ;-)

Voir aussi mon tutorial pour les détails, comment faire une plainte à l'adresse suivante :

Spamfight
http://www.webwizardbiz.com/tutorials/security/spamfight/

Glossaire :

F.A.I. : Fournisseur d'Accès Internet
I.S.P. : Internet Service Provider
SPAM : Courrier non sollicité, ou *pourriel* au Canada
Adresse IP : La plaque généalogique de notre PC
IP Spoofing : Falsification de l'adresse IP
Phishing : Détournement d'un site Internet
Toile = Internet
Malware : Mot regroupant les bestioles informatiques (vers, virus, troyen, etc.)
Tutorial : Didacticiel, cours
MAJ : Mises Á Jour

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