Internet Monitor Security News Bulletin

EDITO

Bonjour, chers internautes

Dans cette édition du bulletin 01/2004 de l'Internet Monitor (http://www.internetmonitor.lu), vous trouverez une sélection des informations de la sécurité PC & Internet les plus relevantes, ainsi que des tutoriaux (Cours online GRATUITS).

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

Éditorial : L'évolution technique et la société

Gust MEES

La technique (Internet, PC, audio et vidéo), plus clair, les mass médias évoluent tellement vite (courbe exponentielle) que la société (nous-même) n'arrivons plus à suivre parallèlement !

Ceci a des conséquences sur notre vie sociale et à l'éducation de nos enfants. Comment éduquer nos enfants aux dangers de l'Internet, quand nous-même, les parents, ne les connaissent pas ?

Est-ce que un moment donné, réflexion faite, l'état ne devrait intervenir ?

Pourquoi l'état ?

L'éducation de nos jours prépare nos enfants aux connaissances nécessaires pour les préparer au monde du travail, pour leurs donner une chance de réussir dans le monde du travail.
C'est la formule ancienne, qui a été appliquée à l'époque où il n'y avait que le père qui travaillait pour gagner le pain quotidien.

Mais de nos jours il y a égalité des chances et rares sont les couples qui ne travaillent tous les deux (presque impossible du point de vue financier). Ces couples doivent en même temps élever leurs enfants (tâche difficile) et de les préparer pour leur vie.

Nul, n'a plus le temps de suivre, de s'informer et de réagir pour suivre l'apprentissage des nouvelles technologies (TIC).

Comment alors transmettre nos expériences à nos enfants quand nous n'avons pas nous même les connaissances nécessaires ?

Mission impossible !

Petite idée :

Ne serait-il pas possible (nécessaire) d'inclure dans les programmes de l'école des cours spécifiques à la matière ?

Appelons les *Éducation aux TIC*.

Petite rétro perspective:

Je me rappelle ma jeunesse comme étudiant dans l'enseignement secondaire technique ; à l'époque (1970) j'avais quinze (15) ans ; c'était le *boom* des télévisions, un nouveau mass média ; le mot mass média fût créé !

On nous enseignait comment traiter d'une manière critique les informations multiples, que nous procurait ce nouveau média et en plus on nous enseignait comment l'utiliser !
Merci, Madame SALENTINY, j'ai retenu le contexte de tes cours à ETTELBRUCK (LU) !
Spécialement on nous enseignait à ne pas devenir dépendant de la télé, comment faire le choix des programmes et comment l'utiliser pour nos études.

Á l'époque, comme c'était nouveau, cela fût quand même des masses d'informations auxquelles nous étions exposées en une fois et auxquelles notre cerveau n'était pas habitué (pas encore). Il fallait quand même digérer toutes ces informations, il fallait s'habituer, donner le temps au cerveau d'assimiler les informations et de multiplier les neurones pour élargir la capacité de réception des données.

Je crois, que maintenant, nous sommes dans une situation pareille. Le PC ensemble avec Internet font belle paire et ont créés un nouveau mass média !

Personnellement, je trouve que, ce serait désirable d'introduire une section *Éducation aux TIC* dans l'enseignement primaire et aussi à prévoir des soirées d'informations avec le même contenu pour le grand public (parents et seniors) dans des locaux des communes.

Lire aussi mes articles suivants :

Le PC, Internet et son utilisationhttp://www.internetmonitor.lu/index.php?action=article&id_article=67449&id_rubrique=8949
Nos responsabilités dans Internet
Guide pratique de la sécuritéhttp://www.internetmonitor.lu/index.php?action=article&id_article=67355&id_rubrique=8949
L'irresponsabilité dans Internet et comment réagirhttp://www.internetmonitor.lu/index.php?action=article&id_article=67399
Introduction à la sécurité (pdf)http://www.internetmonitor.lu/download/Fiche_technique_Securite.pdf

Comme Internet évolue très vite, c'est entre temps devenu un monde virtuel, qui vient tout juste de sortir de ses souliers d'enfants (stade de Teenie), les applications qui vont suivre sont encore beaucoup plus vastes.

Essayez de comparer Internet (le monde virtuel) avec notre monde réel, pour voir qu'elles applications seront encore possibles ; c'est à prévoir sans être un prophète !

Visual Internet

Exemples existants :

E-mail : Courrier (P&T), lettres
Chat : Conversations entre des groupes de personnes
Blog : Journal intime (FR), Tagebuch (DE), Diary (EN)
Pop up : Courrier publicitaire inséré dans les journaux et magazines
SPAM : Envoi de courrier non sollicité dans la boîte aux lettres (réclames, publicités)
PHISHING : Falsification de documents pour avoir un contrat et voler de l'argent
Moteurs de recherche (Google etc) : Bibliothèques
Site Internet (homepage) : Maison ou appartement loué
Hosting : Loyer dans le monde virtuel
Propre serveur : Propre maison
Trojan : Facteur clandestin
Virus : Épidémies transmises d'une personne à l'autre
Voice over IP (VOIP) : Téléphonie
Dialer : Voleur de grands chemins (FR), Wegelagerer (DE), High Way Man (EN)
E-commerce : Commerces
E-banking : Banques
Anti-virus : Vaccin contre les maladies
Firewall (pare feu) : Système d'alarmes
Webcam : Voyeurisme

L'Internet (le monde virtuel) est une copie exacte du monde réel et de nos caractères !

À vous maintenant de réfléchir ce qui pourrait arriver encore ?
Copyright by Gust MEES (LU)

Phishing (FR) : Les arnaques bancaires se multiplient dans le monde

Gust MEES

Au cours des dernières semaines, des campagnes d'escroquerie par courriel de type «phishing» et d'autres fraudes ont été lancées contre les clients de plusieurs banques dans le monde.

Si les campagnes de «phishing» semblaient d'abord dirigées vers les clients de banques américaines et de commerces en ligne tels qu'Ebay et Paypal, les pirates élargissent maintenant leur auditoire en s'attaquant à une plus grande variété d'institutions financières.

La semaine dernière, les médias révélaient que quelques clients de banques françaises (Société Générale et Bred) ont constaté que des fonds avaient été détournés de leur compte bancaire. Les fraudeurs responsables de ces détournements étaient en possession des noms d'utilisateur et mots de passe des victimes, probablement à la suite d'une campagne de «phishing».

Depuis quelques jours, c'est au tour des internautes allemands d'être la cible d'arnaques par courriel qui tentent de soutirer des informations confidentielles aux clients de la Deutsche Bank et de Postbank. Des pirates asiatiques seraient à l'origine de cette attaque qui, de l'avis de porte-parole de ces institutions financières, manquerait toutefois de «professionnalisme».

En Amérique du Sud, le cheval de Troie Banker tente depuis quelques semaines de dérober aux clients de banques brésiliennes les données d'identification requises pour ouvrir une session en ligne.

Même le petit marché du Québec a déjà connu quelques tentatives de fraude, notamment, l'automne dernier, le soi-disant concours qui tentait de subtiliser les numéros de cartes de crédit et mots de passe de clients de Desjardins et BMO.http://benefice-net.branchez-vous.com/nouvelles/03-09/07-293703.html

Vous pouvez vous familiariser avec les fraudes par courriel de type «phishing» en passant un test en ligne qui contient des messages frauduleux déjà propagés sur Internet. Afin de vous protéger contre ces arnaques, il est vivement recommandé de ne pas saisir d'informations personnelles dans des formulaires qui arrivent par courriel et de ne pas ouvrir de session à partir d'un lien fourni dans un message. http://www.branchez-vous.com/actu/04-07/08-257303.html
Source de l'article: BRANCHEZ VOUS (CA)
http://www.branchez-vous.com/actu/04-08/08-276104.html

Security News (FR) : Un PC sans protection ne survivrait que 20 minutes sur Internet

Gust MEES

Selon les données de l'Internet Storm Center (ISC), les PC sur lesquels on n'a pas encore appliqué les correctifs d'importance critique pourraient maintenant se faire infecter en 20 minutes, pour peu qu'ils soient connectés à Internet.

Le «temps de survie» de 20 minutes est calculé comme «le temps moyen entre les incidents rapportés par une adresse IP typique». Comme l'ISC considère que la plupart de ces incidents sont générés par des vers informatiques qui tentent d'infecter un système, cette période correspondrait au temps moyen pour la contamination d'un ordinateur ne disposant pas d'une protection minimale, notamment les correctifs pour les failles jugées critiques.

Cette diminution du «temps de survie» inquiète l'ISC car s'il devenait inférieur au temps nécessaire pour télécharger les mises à jour critiques nécessaires à sa protection, un nombre important de nouveaux PC pourraient par exemple ne pas «survivre» à leur première connexion à Internet.

L'ISC indique toutefois dans sa page sur l'historique du «temps de survie» qu'il existe une grande variabilité dans ces temps d'un réseau à l'autre et, en observant le graphique, on peut aussi constater que ces temps varient considérablement à l'intérieur des périodes d'un mois.

http://isc.sans.org/survivalhistory.php

Toujours sur le site de l'ISC, on peut aussi remarquer sur cette carte mondiale que Dabber et Sasser, des vers informatiques qui se propagent sans intervention humaine et qui peuvent donc infecter des PC vulnérables lors d'une simple connexion à Internet, sont encore très actifs, en particulier en Asie.

Source de l'article: BRANCHEZ VOUS (CA)

http://www.branchez-vous.com/actu/04-08/08-274904.html

http://isc.sans.org/large_map.php

Phishing (DE) : Phishing wird zum Volkssport unter Ganoven

Gust MEES

Alarmierende Erkenntnisse bringt eine neue Studie des Marktforschungsinstituts Gartner: Danach werden immer mehr Konten- und Kreditkartendaten ausgespäht.

Dieser Kriminalitätszweig, zu dessen schlagzeilenträchtigsten Spielarten das „Phishing“ im Internet gehört, hat in den vergangenen zwölf Monaten in Amerika einen Schaden von 2,4 Milliarden US-Dollar verursacht. 1,98 Millionen US-Amerikaner seien Opfer eines solchen Betrugsversuches geworden – mit einem durchschnittlichen Schaden von 1.200 US-Dollar.

Mit der neuen Erhebung bestätigt Gartner die Erkenntnisse einer eigenen Untersuchung aus dem Monat Mai zum Thema Phishing. Hierunter versteht man den Versuch, von Websurfern über täuschend echt aussehende Unternehmensseiten – insbesondere von Geldinstituten – Kontoinformationen wie beispielsweise die Geheimnummer zur Kreditkarte zur erfragen. Gartner fand seinerzeit heraus, dass zwischen Mai 2003 und Mai 2004 sagenhafte 57 Millionen US-Bürger mindestens eine Phishing-E-Mail erhalten haben. Beispielsweise gab der Absender vor, von der Citibank zu kommen und bat, auf einer speziellen Seite die Kontoinformationen zu aktualisieren – mit Online-Banking-Passwörtern.

In der aktuellen Studie weisen die Autoren den Medienberichten zufolge darauf hin, dass neben der Phishing-Gefahr auch das Keystroke-Logging rapide an Bedeutung gewinne. Hierbei wird durch Viren oder Spammails eine so genannte Spyware auf dem Rechner von Betroffenen platziert, die anschließend sämtliche Tastatureingaben protokolliert und an eine Webseite weiter leitet. Die Auswertung dieser Daten liefert in vielen Fällen Rückschlüsse beispielsweise auf Passwörter.

Inzwischen hat der Bereich „Kontospionage“ bei den Betrugsdelikten in Sachen Häufigkeit den zweiten Rang erobert. Nur der tatsächliche Diebstahl von Kreditkarten komme noch häufiger vor.

Quelle des Artikels: PC GO (DE)

Exhibitions (EN) : INSIDE ID CONFERENCE & EXPO

Gust MEES

Inside ID Conference & Expo helps define and nurture the evolving discipline of modern identity management, covering some of the most pressing challenges of our uncertain world including: digital identity, homeland security, identity theft and financial transaction fraud. The event provides forums for interaction among diverse constituencies dealing with sensitive issues such as privacy, cross-credentialing, and federated identification. Also, there is no better place to learn about and experience solution-enabling technologies such as public key cryptography (PKI), biometrics, RFID and smart cards.

=> INSIDE ID CONFERENCE & EXPO 2004's top-rate program has been developed around three track themes and dives deeper with additional sessions in these topic areas. Visit the Web site for

speaker and session descriptions:

ENTERPRISE IDENTITY MANAGEMENT TRACK

THE STATE OF IDENTITY MANAGEMENT: THE NEED AND THE MARKETPLACE
IN-DEPTH SESSIONS INCLUDE:
- Identity Management: Emergence of a Discipline
- The Business of Identity Management: Evolution of the Marketplace
- Identity-Driven Security for On Demand Business

AUTHENTICATION: THE FRONT END OF SOUND IDENTITY MANAGEMENT
IN-DEPTH SESSIONS INCLUDE:
- Identity Management Policy in the Modern Enterprise
- Knowledge-based Authentication Services
- Open Authentication: Providing Interoperable Identity Credentials
- Success Factors in Integrated Identity Management

FEDERATED IDENTITY: THE QUEST FOR INTEROPERABILITY
IN-DEPTH SESSIONS INCLUDE:
- The Quest for Interoperability in Federated ID
- WS-I: Ensuring Interoperable Secure Web Services
- Interoperability Specifications with SAML

MODELS OF FEDERATED ID AND WEB SERVICES
IN-DEPTH SESSIONS INCLUDE:
- Understanding Variations in Identity Federation Models
- Microsoft's Approach to Identity Management from ADFS to Web SSO
- Liberty Alliance: Building a Critical Mass
- The Electronic Authentication Partnership: Business Process,Governance and Compliance

BUSINESS CASES AND CASE STUDIES IN IDENTITY MANAGEMENT
IN-DEPTH SESSIONS INCLUDE:
- Identity Management in the Mobile World
- Johnson & Johnson's Worldwide PKI Implementation
- Using Digital Certificates at Wells Fargo
- e-Authentication Case Studies: Deploying Federated ID
- Deploying Large-scale Digital Identities for the Pharmaceutical Industry Worldwide: The SAFE Project

GOVERNMENT ID APPLICATIONS TRACK

ID THEFT AND FINANCIAL FRAUD
IN-DEPTH SESSIONS INCLUDE:
- Identity Theft & Financial Fraud Trends
- Financial Fraud: Recent Schemes, Cases and Stats
- The Changing Face of Identity Theft: Beyond the Phishing Phase
- Initiatives for Protecting Financial Institution Customers
- Technologies and Best Practices for Fighting Identity Theft

HOMELAND SECURITY APPLICATIONS
IN-DEPTH SESSIONS INCLUDE:
- U.S. VISIT: The Identity Management Mega Project
- The Transportation Worker ID Card: Bringing Trust to the Transportation Infrastructure
- The Maritime Administrative Card: Credentialing and Work Record Applications
- Implementing DHS Employee Credentialing

ID CARD APPLICATIONS FOR PHYSICAL & LOGICAL ACCESS
IN-DEPTH SESSIONS INCLUDE:
- The NASA Employee Credential: An Integrated Solution
- Smart Card Enabled Physical Access for Cross Agency Interoperability
- RFID: Meeting Modern Security Needs

ID IN THE DOD
IN-DEPTH SESSIONS INCLUDE:
- DoD's Solution Set for Personal Identity Protection
- Integrating Biometrics with the CAC Card
- Panel Discussion: Cross Credentialing: On the Fast Track at DoD

LARGE-SCALE GOVERNMENT ID
IN-DEPTH SESSIONS INCLUDE:
- The U.S. Passport: Transitioning to e-Passports
- Improvements in Drivers Licensing
- Around the World With Large Scale ID

TECHNOLOGIES AND POLICIES TRACK

BIOMETRIC TECHNOLOGY
IN-DEPTH SESSIONS INCLUDE:
- Biometric Products, Trends, and Applications
- DoD Biometric Interoperability Challenges
- Biometric Standards: Sublime, Sexy or Superfluous?
- Balancing Scalability and Accuracy in Large-Scale Biometric Systems
- Coordinating the Government's Biometric R&D Efforts

CARD TECHNOLOGY

IN-DEPTH SESSIONS INCLUDE:
- The Current & Future State of ICs Used in Smart Cards
- Chip Cards: The Key to Robust Security
- Providing the Platform for Multi-Application Smart Cards
- Practical Implications of Putting Multiple Technologies on Cards
- Processing Power in your Pocket: Why Form Factor Matters

PRIVACY AND POLICY
IN-DEPTH SESSIONS INCLUDE:
- Defending and Building Privacy in the Digital Age
- Achieving Data Integrity, Privacy and Interoperability at DHS
- Code of Principles for the Acceptable Use of Biometric Technology Purposes
- Privacy Perspectives on Travel Document Standards

ID DATABASES AND PROOFING
IN-DEPTH SESSIONS INCLUDE:
- The Privacy Implications of Data Proofing
- Advanced Systems for Detecting and Reducing Identity Fraud
- Complying with the U.S. Patriot Act: Know Who You Are Doing Business With
- The Benefits of a Full Positive Database

DOCUMENT SECURITY
IN-DEPTH SESSIONS INCLUDE:
- TBA

1-Day, 3-Day and FREE Expo Pass Registration Available Now at:
http://www.jupiterevents.com/insideid04/registration.html
Please Enter Priority Code: 81IDN8 in the space provided during online registration

SPONSORS/EXHIBITORS OF INSIDE ID CONFERENCE & EXPO 2004 INCLUDE:

PLATINUM-PLUS SPONSOR: Hewlett-Packard Company
GOLD SPONSOR: ChoicePoint
EXHIBITORS: AC Technology; Alacris; Anteon; Axalto; ConnecTerra; CoreStreet; Daon; DMDC - Defense Manpower Data Center; Fargo Electronics; Fingerprint Cards; Gemplus; Giesecke & Devrient; Janus Associates; Magtek; Maximus; Muhlbauer Inc.; Primary Payment Systems, Inc.; Retinal Technology; Role Engineering by Metacom; Sagem Morpho, Inc.; SCM Microsystems,Inc.; Supercom
PARTNERING ORGANIZATIONS: GlobalPlatform; ISTPA - International Security Trust & Privacy Alliance; The Liberty Alliance Project; Smart Card Alliance
MEDIA PARTNER: findBIOMETRICS

Inside ID Conference & Expo is produced by Jupitermedia and is hosted by Inside ID (http://www.insideid.com) - The Source for Advanced Identity Management Solutions & Technology

For information or complete details on exhibiting or any sponsorship opportunity, please contact: Elaine Mershon, Director of Sales, at emershon@jupitermedia.com or at (508) 533-4995.
Program and website InsideID

Security News (DE) : Informationssicherheit in KMU (PME)

Gust MEES

Eine neue Broschüre der gemeinnützigen Stiftung InfoSurance soll kleinen und mittleren Unternehmen (KMU / PME) helfen, die Sicherheit ihrer Informatik zu verbessern.

Die Broschüre mit dem Titel «Mehr Informationssicherheit für KMU (PME)» kann kostenlos von der Website der Stiftung InfoSurance [1] heruntergeladen werden. Sie umfasst ein 10-Punkte-Programm für einen verbesserten Grundschutz der Informationstechnologien in KMUs (PME). In vielen kleinen und mittleren Schweizer Unternehmen ist es laut InfoSurance um die Informationssicherheit schlecht bestellt. Dies sei ein immenses Risiko: Der Verlust von Betriebsgeheimnissen oder vertraulichen Kundendaten könne sich drastisch auswirken. Ohne Computer stehe die Produktion von Firmen Stunden oder gar Tage still. An der Broschüre haben Unternehmen wie Omnisec, Trivadis, Symantec und Infoguard mitgearbeitet.
Quelle des Artikels: Infosurance http://www.infosurance.ch/de/kmu.htm PC TIPP (CH) http://www.pctipp.ch/webnews/wn/28058.asp

Expositions (FR) : 'Confiance et Sécurité' : synthèse et pistes d'avenir, le 28 septembre 2004

Gust MEES

17h-20h (cocktail)
Au Ministère délégué à la Recherche
1, rue Descartes, Paris (5e), amphi Poincaré

Après 8 mois de travail et 5 réunions publiques, la Fing présente la synthèse des réflexions communes aux réseaux de recherche (RNRT, RNTL, RMNT, RIAM), ainsi qu'aux ministères de la Recherche et de l'Industrie, sur le thème de la Confiance et de la sécurité sur les réseaux.

Ordre du jour (à compléter) :

Synthèse des travaux, pistes de recherche : Arnaud Belleil et Daniel Kaplan, Fing
Les programmes de recherche :
Oppidum - Mireille Campana, ministère délégué à l'Industrie
L'ACI "Sécurité informatique" - Claude Kirchner, Loria / Inria

Nouveaux défis, nouveaux enjeux pour la confiance et la sécurité :
Dominique Boullier, Université technologique de Compiègne, directeur du Laboratoire des
usages Lutin (RNRT-CNRS) à la Cité des sciences et de l'industrie

Christian Huitema, Microsoft, architecte du groupe "Windows Networking & Communications" (en visioconférence)
Michel Riguidel, ENST
Georges Kayanakis, ASK
Un autre intervenant à confirmer (biométrie)

Conclusion par un grand témoin

L'inscription en ligne est gratuite mais obligatoire à l'adresse suivante:

Inscriptions: FING (FR / PARIS)
http://www.fing.org/index.php?rubrique=confiance_reunion06

Phishing (DE) : Mangelnde Online-Sicherheit bei Finanzinstituten

Gust MEES

Die Webseiten verschiedener Banken in Deutschland sind nicht ausreichend gegen Manipulationen geschützt. Das vereinfacht das Ausspähen von Kontodaten durch so genannte Phishing-Attacken. Online-Bankkunden sollten die Web-Adressen, auf denen Nutzerdaten abgefragt werden, nur direkt eingeben oder über ihre Lesezeichen ansteuern. 2003 wurden nach Ergebnissen eines Marktforschungsinstituts rund zwei Millionen Online-Bankkunden durch gefälschte Überweisungen im Schnitt um 1200 US-Dollar geprellt.

Im ersten Halbjahr 2004 haben solche Betrugsversuche um 1200 Prozent zugenommen. Das Ausspähen von Kontodaten und PINs wird inzwischen weitaus professioneller ausgeführt und lässt vermuten, dass es sich längst um organisierte Kriminalität handelt. Per E-Mail locken Betrüger Nutzer auf gefälschte Webseiten, die den Webseiten der Banken täuschend ähnlich sehen. Waren diese Phishing-Mails bis vor kurzem noch vergleichsweise dilettantisch, können sie inzwischen sogar IT-Fachleute täuschen. So zeigen die gefälschten Seiten das Schlosssymbol als Zeichen für eine sichere Verbindung an - real handelt es sich aber nur um eine eingebaute Grafik.

Die Banken haben die Schuld bisher meist auf die Unvorsichtigkeit der Anwender geschoben. Doch das ist nur die halbe Wahrheit. "Es hat sich auch gezeigt, dass nicht alle Banken vorhandenes Programmierwissen nutzen, um ihre Web-Seiten möglichst sicher zu gestalten", erläutert c't-Redakteur Holger Bleich. Einige Banken gestalten ihre Webseiten immer noch mit unsicheren Frames: oben ein Titel, rechts die Navigation und in der Mitte der eigentliche Inhalt. Doch bereits seit sechs Jahren ist bekannt, dass sich durch Sicherheitslücken nahezu aller Browser einzelne Frames überschreiben lassen. Außerdem hat sich gezeigt, dass Anwendungen, mit denen sich Eingaben machen lassen, nicht ausreichend auf mögliche Manipulationen geprüft wurden.

Webseiten, die persönliche Informationen abfragen, sollte man grundsätzlich nur über seine Lesezeichen oder durch manuelle Eingabe ins Adressfenster des Browsers abrufen, empfiehlt die c't-Redaktion Surfern. Auf Links in E-Mails oder anderen Webseiten sollte man sich in solchen Fällen niemals verlassen.

Quelle des Artikels: FREELETTER (DE)
http://www.freeletter.de/cgi-bin/news/news.cgi?newsid1091871758,74272

Microsoft News (FR) : Le service pack 2 de Windows XP est enfin prêt

Gust MEES

Dans un premier temps, Microsoft a expédié la version finale de la mise à jour de son système d'exploitation aux fabricants de PC et, dans quelques jours, les internautes pourront commencer à la télécharger.

Microsoft Canada indique que la version finale du service pack 2 sera lancée au Québec le mercredi 11 août. Les internautes qui désirent le télécharger dès qu'il sera disponible peuvent dès maintenant activer la fonction de mise à jour automatique de Windows XP. Pour ce faire, il suffit de suivre les instructions détaillées qui figurent dans cette page du site de Microsoft. http://www.microsoft.com/france/securite/protection/windowsxp/updates.asp

Le service pack 2 de Windows XP est une mise à jour que les

spécialistes considèrent comme très importante car elle renforce considérablement la sécurité informatique, notamment grâce à l'activation par défaut du coupe-feu intégré au système, à un regroupement de fonctions relatives à la sécurité dans le tout nouveau «Centre de sécurité Windows» et à l'activation de certaines fonctionnalités, intégrées au coeur de certains processeurs, qui visent à empêcher les exploitations de failles par un dépassement de la mémoire tampon.

Microsoft indique également que le SP2 pourra éventuellement être commandé gratuitement sur cédérom à partir de son site Web, une option pratique pour les internautes qui possèdent un accès Internet à faible débit ou qui préfèrent en avoir une copie sous la main en cas où ils devraient réinstaller leur système d'exploitation.

Source de l'article: BRANCHEZ-VOUS (CA)
http://www.branchez-vous.com/actu/04-08/08-272702.html

Security News (FR) : Des pirates paralysent des centaines de sites à l'aide d'un réseau de zombies

Gust MEES

Des pirates informatiques ont attaqué les serveurs de Doubleclick, un très important fournisseur de bannières publicitaires sur Internet aux États-Unis, ce qui a eu pour effet de perturber et ralentir les quelque 900 sites qu'il alimente.

Les pirates auraient utilisé un réseau de PC «zombies», c'est-à-dire préalablement infectés par un ver informatique ou un cheval de Troie, afin de lancer des attaques par déni de service vers les serveurs DNS de Doubleclick qui se trouvaient ainsi paralysés.

Hier, pendant près de quatre heures, environ 900 sites Web américains très fréquentés (CNN, Washington Post, New York Times, etc.) ont ainsi éprouvé des problèmes d'affichage de leurs pages Web et des ralentissements.

Ces attaques seraient similaires à celles qui ont été lancées contre Akamai le mois dernier (lire la nouvelle Panne de Microsoft et Google: vous avez peut-être participé à l'attaque), et qui ont paralysé temporairement des sites Web très fréquentés tels que ceux de Google, Yahoo et Microsoft.
http://www.branchez-vous.com/actu/04-06/08-234702.html
Source de l'article:

Phishing (FR) : Phishing, le nouveau fléau d'Internet

Gust MEES

Après le courrier non sollicité (SPAM), que l'on surnomme le fléau d'Internet, une autre pratique informatique malveillante est en bonne voie de surpasser le SPAM et ceci avec une vitesse incroyable, le PHISHING !

PHISHING = USURPATION D'IDENTITÉ

Le *PHISHING* c'est de l'escroquerie. C'est une arnaque qui est pratiquée en envoyant un courrier électronique (email), portant la signature (logo) d'une banque, d'un FAI (ISP) ou d'un cyber - commerçant (e-commerce). Donc, à première vue, des courriers électroniques (email) semblant être confiants.

Ces courriers électroniques (email) contiennent un lien (link), pointant envers un site Internet du soit disant établissement.
Dans ces emails on vous demande de cliquer le lien (link) et de suivre les instructions sur ce site Internet.

En plus, on vous explique que du à une panne informatique, la base de données du dit établissement a été corrompue et que vous devez à nouveau fournir toutes vos données personnelles et confidentielles (mot de passe, login, numéro carte bancaire etc).
Quand vous cliquez le lien, vous serez redirigés vers un site Internet tout à fait identique à celui du dit établissement.

En plus, dans le champ d'adresse de votre navigateur (Internet Explorer, Netscape, Opera, Mozilla, Firefox etc) vous allez voir aussi, l'adresse exacte. (URL)

On vous demande maintenant de remplir un formulaire. Surtout ne le faites pas, vous donneriez toutes vos données secrètes aux truands.

Ce que vous voyez maintenant, c'est un site Internet dupé, un site web truqué. On appelle ceci aussi du *IP SPOOFING*.

BSI (DE) http://www.bsi.de/fachthem/sinet/vulner/g5048.htm

COMMENT CA MARCHE (FR)
http://www.commentcamarche.net/attaques/spoofing.php3

Les escrocs ont copié le site Internet et vos données seront envoyées envers ces escrocs, qui se feront le plaisir de dérober votre argent !

!!! Et surtout ne cliquez pas ce lien !!!
En cliquant le lien, il se pourrait qu'automatiquement on vous installe un *TROJAN* contenant un *KEYLOGGER* sur votre PC !
Un *KEYLOGGER* est un programme qui enregistre toutes vos actions (chaque touche frappée) et par l'intermédiaire du cheval de Troie (TROJAN), envoie ces données à son programmeur.

Sachez que les banques (e-banking) et les cyber-commerçants (e-commerce) ne vous enverront jamais un courrier électronique (email) pour vous demander de leurs fournir à nouveau vos données personnelles !

Sont connus actuellement comme victimes du PHISHING, la CITIBANK et EBAY.
D'autres ont été victime certainement, mais craignent de le révéler, ayant peur pour leur renommée.

Glossaire :

FAI = Fournisseur d'Accès Internet
ISP = Internet Service Provider
IP = Internet Protocol
Adresse IP = adresse de votre PC (Ex. : 194.54.212.53) = similaire à votre plaque d'immatriculation de votre voiture
IP – SPOOFING = Usurpation d'adresse IP
KEYLOGGER = Programme enregistrant toutes activités sur le PC (chaque touche enfoncée sera enregistrée)

Tutoriaux (Cours gratuits) : Le PC, Internet et son utilisation

Gust MEES

Nous vivons une époque, où nous avons l'habitude d'utiliser du matériel technique et du matériel électronique (TV, télécommande, DVD, CD etc…).

Avec ce matériel nous ne nous soucions pas pour l'utiliser.
Nous l'utilisons, nous n'avons pas besoin d'avoir des connaissances spéciales, ni de prendre des précautions spéciales, ni de nous instruire (apprendre, informer).

Maintenant, est apparu l'ordinateur (PC + MAC) et Internet. Ces deux inventions, font belle paire ensemble et ils sont en train de faire une révolution informatique.
Nous vivons une époque nouvelle, l'époque de la communication et de l'information (TIC).

Soudain, avec ce matériel technique (PC + MAC) et cette application (Internet), nous ne pouvons plus simplement les utiliser sans nous instruire et de nous informer !

Une application technique (Internet + PC) qui nous force à connaître les bases de la sécurité informatique et les bases de fonctionnement de l'Internet.

En plus de ceci il nous faut apprendre le maniement du PC (prendre des cours ou apprendre comme autodidacte) !

Avec la révolution informatique c'est le *LIFE LONG LEARNING* qui s'annonce !

Une éducation à Internet s'impose. Internet n'est pas un joujou, mais un outil de travail précieux et une source d'informations inépuisable, utilisé simultanément par des millions d'internautes.

Mais ces outils ont besoin d'entretien et de maintenance, tel qu'une voiture.

Voir aussi mes articles suivants :

Nos responsabilités sur Internet (http://www.webwizardbiz.com/tutorials/responsabilites)

Guide pratique de la sécurité PC & Internet (http://www.webwizardbiz.com/tutorials/guidesecurite)

Nous aussi, nous avons besoin d'une éducation à l'Internet. Nous devons apprendre à respecter le code éthique de l'Internet, la nétiquette, la chatiquette et le plus important, la sécurité sur Internet.

Eh bien oui, comme vous pouvez le constater maintenant, la révolution informatique nous impose à apprendre.

Mais est-ce que cela ne vous rappelle pas quelque chose ? Par exemple l'apprentissage pour faire le permis à conduire ?

Cela a fait clic chez vous ? Vous voyez les points communs ? Non ? Je vous les explique.

Nous avons du apprendre :

1. Code de la route
2. Responsabilités envers les autres
3. Le maniement technique de la voiture
4. La sécurité (priorité, freins, contrôle technique, rétroviseur, miroirs latéraux…

Pourtant, aujourd'hui, nous ne pouvons nous imaginer une vie sans voitures. En plus quand nous passions le permis à conduire nous avons du faire un examen.

Heureusement, pour surfer sur Internet, nous n'avons pas besoin de permis, mais néanmoins il nous faut apprendre que quand nous naviguons sur Internet, nous sommes connectés avec des millions d'autres internautes en même temps et qu'il faut observer à ne pas blesser la communauté.

RESPECTER QUELQU'UN D'AUTRE = AUSSI RESPECTER SOI-MÊME !

Blesser la communauté ? Oui, par exemple si nous avons un virus sur notre PC, nous le refilons aussi aux autres internautes. Nous infectons les autres internautes ! Une épidémie de virus se propagera sur toute la toile (Internet) !

Il faut essayer à ne pas seulement penser à nous même, mais à développer un esprit de communauté.

Lire aussi mon article :

Nos responsabilités sur Internet (http://www.webwizardbiz.com/tutorials/responsabilites)

Protection des mineurs (FR) : *Le fossé juridique*

Gust MEES

Il y a peu de temps et même encore maintenant, nous parlions d'un * fossé numérique *, lequel est en train de devenir plus étroit et même qui disparaîtra dans le proche futur.

Les ordinateurs (PC & MAC) commencent tout doucement à s'établir dans tous les ménages et deviendront bientôt indispensables à notre vie quotidienne, forcément puisque nos enfants les utilisent et les utiliserons aussi à l'école.
De même, le PC envahi les bureaux des entreprises et trouver un emploi sans connaissances de base informatique est devenu très difficile, à voir illusoire !

240.000.000 d'ordinateurs Source WIKIPEDIA http://de.wikipedia.org/wiki/Internet sont actuellement connectés au réseau des réseaux (Internet) ; un chiffre énorme, lequel ne cesse d'augmenter.

Comme Internet est décentralisé (n'appartient à personne et à tout le monde), en plus pas gouverné (pas encore) et sans hiérarchie (l'idée de départ d'Internet), presque tout est permis et rien n'est défendu !

Néanmoins des propositions pour la gouvernance d'Internet sont en cours par la *Société pour l'Information* ainsi que de l'ISOC et de l'ISOC France.

ITU http://www.itu.int/wsis/docs2/pc1/doc5-fr.doc
ISOC http://www.isoc.org/news/pdfs/isocnews-9.pdf

ISOC FRANCE http://www.isocfrance.org/edito/index.php?ID=873&PHPSESSID=6538392f760655876a0de3cd6cbe2593

Cette décentralisation et l'esprit libre du début d'Internet, nous ont apporté aussi pas mal de problèmes du point de vue de criminalité sur Internet. Des programmeurs de virus (chevaux de Troie, vers, phishing, spoofing et cie), des pédophiles, des truands, des affaires commerciales illégales font légion sur Internet et ne sont pas combattables efficacement pour l'instant ! Il n'existe presque pas de lois pouvant combattre ces délits et en plus les lois ne sont pas pareilles dans tous les pays.

Entre temps il y a un * fossé juridique *, qui s'est créé, lequel qu'il faudrait maintenant essayer d'éliminer ou au moins essayer de le réduire à un minimum. Lire aussi mon article :

Carte d'identité virtuelle http://www.internetmonitor.lu/index.php?action=article&id_article=65263

Quand je parle de * fossé juridique *, je pense en premier lieu aux enfants et surtout aux mineurs.
Pour l'instant, il n'existe pas de contrôle fiable pour que les enfants

n'accèdent pas aux sites pornographiques et de violence, ni les sites de sectes,de haine, de racisme…
Quand nous voyons la croissance des actions de pédophilie sur Internet, ceci devrait faire réfléchir !
Récemment, au Luxembourg, il y a eu arrestation de 16 pédophiles !!!

Seize (16) pédophiles, pour une population de 440.000 habitants seulement, dont selon les derniers sondages, 50 % des ménages seraient connectés à Internet, c'est un chiffre énorme et alarmant, mais aussi seulement la pointe de l'iceberg !

Le slogan * fossé juridique * pour Internet devrait se mémoriser dans nos têtes et surtout dans les têtes de nos politiciens.
Certains pays ont déjà eu le courage de réagir en matière de législation, à voir certains états des États-Unis :

NETFAMILY NEWS http://www.netfamilynews.org/nl020315.html

Pennsylvania ISPs & child porn
According to BNA Internet Law, Pennsylvania has enacted a new anti-online child porn law that may require local ISPs to block access to such content or face criminal prosecution. House Bill 1333 requires ISPs to remove or disable access to child pornography within five days of notification by the state attorney general. It will be interesting to watch this development to see if it's precedent-setting in the United States. Here is the legislation (in pdf format).
Traduction:
La Pennsylvanie a décrété une nouvelle loi pour combattre la pornographie avec des enfants en ligne. Cette loi peut exiger des ISP (FAI) locaux de bloquer l'accès à un tel contenu ou de faire face à la poursuite criminelle. House Bill 1333 exige des ISP (FAI) d'enlever ou neutraliser l'accès à la pornographie d'enfants dans les cinq jours de l'avis par le mandataire d'état. Il sera intéressant d'observer ce développement pour voir si cette action sera aussi employée par les autres états aux Etats-Unis. Voici la législation (dans le format de pdf). Législation http://www2.legis.state.pa.us/WU01/LI/BI/BT/2001/0/HB1333P3184.pdf

Il faut tout faire pour protéger nos enfants ! (Notre futur, le futur du monde réel, le futur du monde virtuel)

Internet n'est plus seulement une place de communication et d'échange d'idées, mais Internet est devenu un monde virtuel, un outil précieux indispensable et ouvert à tout le monde.

Internet est devenu un environnement qui implique des conséquences sur notre vie réelle, qui va changer notre économie et notre mode de vie.

Nous vivons dans un monde qui nécessite des réactions et actions rapides, notre temps (nous en avons plus assez déjà) est devenu très précieux.

Internet nous donne cette opportunité ; réagir plus vite, parce que nous recevons nos informations plus vite à travers Internet.

Un outil (PC) que nous utilisons et que nous utiliserons (surtout nos enfants) encore beaucoup plus dans le futur, doit nous donner la sécurité et la confiance.

Mais, vu la décentralisation d'Internet (pas d'hiérarchie), ceci pose des problèmes. Internet n'a pas de frontières, mais chaque pays se veut être maître de son territoire et fait ce qui bon lui semble.

Pour que Internet puisse fonctionner avec une seule législation, valable partout au monde et pour tous, il faudrait une
GLOBAL GOVERNANCE.

Pour aboutir à une formule *GLOBAL GOVERNANCE* la souveraineté nationale des états doit disparaître !
Internet n'a pas de barrières, ni de frontières. Ces barrières sont dans nos têtes et il faut essayer de les démonter petit à petit avec une éducation à l'Internet. Voir aussi mon article :

Education à l'Internet http://www.internetmonitor.lu/download/Fiche_technique_Securite.pdf

Il faut agir, maintenant. Le futur, c'est nos pensées et actions d'aujourd'hui !

ISOC BULLETIN NR.7 (11/2003)
An open debate is now needed to move towards common, globally acceptable policies, processes and technologies to prevent misuse of the Internet. Governments have a vital role to play here as a concerted effort on the part of the Internet community,

non-governmental organisations and Governments can help strengthen and extend today's successful coordination processes.
Traduction:
Une discussion ouverte est maintenant nécessaire pour se déplacer vers un terrain d'entente commun des politiques, des processus communs et globalement acceptables et des technologies pour empêcher l'abus de l'Internet. Les gouvernements ont un rôle essentiel à jouer ici comme effort concerté de la part de la communauté d'Internet, les organisations non gouvernementales et les gouvernements peuvent aider à renforcer et prolonger des processus de coordination réussis d'aujourd'hui.
Notices personnelles :

D'ailleurs, personnellement, je suis d'avis que les lois morales (qui ne sont légalisées), devraient faire part du catalogue des lois de tout pays !
L'humanité a eu besoin de siècles pour construire une civilité basant sur des lois morales, ne les détruisons pas en ne plus tenant compte d'elles !

Veuillez trouver ci-dessous quelques liens intéressants se rapportant à la *Global Governance* :

Sommet mondial de la société de l'information

http://www.itu.int/wsis/docs2/pc1/doc5-fr.doc

http://www.itu.int/wsis/docs/geneva/civil-society-declaration-fr.pdf

Sécuriser Internet pour avoir plus de confiance

http://www.internetmonitor.lu/index.php3?action=page&id_art=80744

Confiance et Sécurité

http://www.fing.org/confiance/

http://www.netfamilynews.org

http://www.saferinternet.org/news/
Copyright by Gust MEES (LU)

Éditorial : Comment nous protéger contre les MALWARE (Virus,Worm,Spam etc...)?

Gust MEES

Sachant que Internet cache quelques dangers de nos jours il faudra accepter aussi que Internet est une aide précieuse laquelle il nous faudra conserver absolument.

Comme c'est impossible (encore) que l'ordinateur soit capable de tout protéger lui-même sans notre aide, nous devrons consacrer nous-même un peu de notre temps précieux pour nous sécuriser.
Mais soyez rassuré(e)s; vous n'êtes pas seul.

Vous pouvez bénificier de tutoriaux online (Internet) et sur le marché il existe une multitude de magazines Pc renfermants et traitants le sujet de la sécurité.

Je vous conseille de vous acheter chez votre marchand de journaux le magazine Pc * L'ordinateur Individuel / Nr.160-Avril 2004* qui traite très bien le sujet de la sécurité avec des propositions de programmes et conseils pratiques.
En plus vous pouvez consulter mon tutoriel (cours gratuit sur Internet) à l'adresse suivante:
Guide pratique de la sécuritéhttp://www.webwizardbiz.com/tutorials/guidesecurite
En espérant de pouvoir contribuer pourque vous puissez vous sentir à votre aise en surfant sur Internet, je vous souhaite bonne lecture, chers internautes et ne perdez pas votre courage.
Il n'y a pas de problèmes, seulement des solutions. Ensemble nous trouverons la solution adéquate!

L'oeil critique : Une carte d'identité virtuelle?

Gust MEES

De plus en plus Internet commence à devenir une trappe pour les internautes. Nous ne pouvons plus nous connecter à Internet sans que le firewall (pare-feu) nous alarme qu'il y a de nouveau quelqu'un qui essaie de pénétrer dans notre PC.
Chaque jour notre boîte à lettres électronique (e-mail) est remplie de courrier non sollicité (SPAM), même avec des filtres anti-spam !

Nous sommes obligés de nous acheter des anti-virus, des firewall et des anti-spyware. Nous sommes obligés de faire la maintenance et les updates pour ces programmes. Ceci nous coûte de l'argent, beaucoup de temps et des nerfs !
Des pratiques commerciales frauduleuses, corruption et les malversations commerciales sont utilisés pour espionner notre comportement de surf afin d'essayer de profiter de nous !
Les mineurs (voir mon article) : Protection des mineurs sur Internet sont recrutés par les pédophiles !http://www.internetmonitor.lu/index.php?action=article&id_article=67423&id_rubrique=9157

Est-ce ceci la liberté promise sur Internet ? Est-ce ceci vraiment le but d'Internet ?
Certes pas, mais existant et sur le point de ne plus être contrôlable. C'est bien d'avoir des chartes d'éthique et de civilité, lesquelles d'ailleurs ne sont pas réglementés mondialement.
Et, qui les connaît ? Vous les connaissez ? Soyez honnête, les aviez-vous déjà vues, annoncées sur le site de votre hébergeur ? Est-ce qu'on vous a déjà dit qu'elles existent ?
Déjà entendu parler de la Nétiquette, de la Chatiquette ?
Sincèrement, j'ai des doutes ! Quand même, pour ceux, qui les connaissent pas, voici des liens informatifs :
NETIQUETTE (DE) , http://www.ping.at/guides/netmayer/netmayer.html#classic
NETIQUETTE (FR) http://www.sri.ucl.ac.be/SRI/rfc1855.fr.html#intro , CHATIQUETTE (DE), http://www.chatiquette.de, CHATIQUETTE (FR) http://www.artetcraft.com/chat/netiquette.php

Mais est-ce que vous croyez que les internautes les respectent ? Malheureusement pas tous, comme vous avez pû le constater vous-même et aussi comme énoncé au début de cet article.
Cette liberté promise a été mal comprise ! Pour avoir droit à une liberté, nous devons d'abord respecter l'être humain, principe fondamental d'une communauté et civilité.
Si nous ne respectons pas les principes de la civilisation, nous la mettons en cause et puis?

Rappelons-nous les bases de la civilisation humaine.

Elle se compose :
Des valeurs traditionnelles d'honnêteté, de courtoisie, de politesse, de civilité, de loyauté, de droiture, de confidentialité et de la protection de l'être humain, surtout de l'enfant !

Est-ce le cas encore sur Internet ? Pouvons nous encore accepter cette démarche vers l'anarchie où tout est permis et rien n'est défendu et ceci en dépit de la civilité ?

Est-ce le retour vers < back to the roots> ou < back to the caves> (Néanderthal et Cromagnon vous saluent) ?

Internet doit changer, sinon ce sera bientôt la mort d'une bonne idée; où la Toile (Web) servira seulement encore aux truands et aux personnes aimant à faire des choses illégales, non morales, nuisibles à la communauté et aux commerçants, essayant de nous vendre leurs produits pour contrer chaque nouveau incident sur Internet !

Est-ce nécessaire ? Est-ce cela la liberté sur Internet ?

Arrêtons de mettre des rustines partout pour raccommoder un produit qui ne répond plus aux exigences des internautes. Ce produit (Internet) a besoin de peau neuve !

Mais qu'est-ce qui pourrait changer ?

Quelques réflexions :

Pensons un peu à la vie réelle, le monde réel, notre monde. Pour arriver à être civilisé, qu'est-ce que nous avons dû changer ? Pour soit disant, forcer l'être humain à respecter certaines bonnes choses, bonnes pour la communauté, qu'est-ce qui a du changer ?
En premier lieu, les lois ! Pour identifier les coupables et protéger les autres, les cartes d'identités !

La carte d'identité virtuelle, appelons la « PUBLIC KEY » (PK) par exemple, serait notre code d'accès pour entrer dans le monde virtuel. Elle contiendrait nos coordonnées privées, telles que :
Date de naissance, pays, fournisseur d ´accès, sexe. Et au cas d'une institution, commerce, écoles etc.., l'adresse, le numéro de registre commercial et le responsable du réseau informatique.

Cette carte d'identité virtuelle (PK) protègera d'abord les mineurs sur Internet, les enfants, notre avenir !
Les sites « XXX », donc à contenu pornographique ne leurs donneraient plus accès à leur site Internet, puisqu'ils seront identifiés par le biais de contrôle de leur identité sur la PK (Carte d'identité virtuelle).

Les spammeurs, fléau de notre siècle, devrons s'identifier à travers cette carte d'identité virtuelle (PK) avant d'envoyer du courrier

électronique (e-mail). Ils perdront le courage de le faire. Ils chercheront un autre moyen ; j'espère qu'ils n'en trouveront pas si vite ?
Mais, soit. Ce problème serait résolu aussi ! Les programmeurs de virus seraient aussi identifiables !

De cette manière, cette carte d'identité virtuelle serait une assurance !

La solution devant nos yeux ?

P.S.: Ce texte sert uniquement à réfléchir (même s'il est un peu radical) et ne se veut pas offensif aux pensées des gens!
Si vous voulez laisser votre opinion, écrivez un petit commentaire en dessous de cet article (Écrire un commentaire)

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