

MySecureIT 2007-2008

Retour d'expérience d'une année de présentations dans des lycées et écoles primaires (environ 130 présentations dispensées à approximativement 5000 enfants et adolescents)

Introduction

Depuis maintenant 3 ans, CASES, structure du Ministère de l'Économie et du Commerce extérieur dédiée à la sécurité de l'information, réalise des campagnes de sensibilisation dans les écoles primaires et lycées du Luxembourg sous forme de présentations. Ces dernières ont pour objectif de sensibiliser les adolescents et enfants aux risques liés à l'utilisation d'Internet. Depuis 2007, le thème du harcèlement perpétré via les nouvelles technologies de l'information et de la communication (cyberbullying) a complété la palette des thèmes abordés lors de cette présentation.

Au cours de ces présentations, généralement très interactives, d'une durée approximative de deux heures, les formateurs de CASES ont recueilli quantité d'impressions et ont documenté certains faits rapportés soit par les élèves soit par les instituteurs ou les professeurs des lycées.

Après un aperçu des définitions de la sécurité et du risque, le formateur explique les objectifs de sécurité (confidentialité, intégrité, disponibilité). Il dresse, alors, un panorama des menaces telles que les virus, les vers, les bots, les spams et le phishing. À cet effet, un film de cinq minutes réalisé par le GovCERT.nl est utilisé comme support pédagogique. Ensuite, le formateur met l'accent sur des menaces plus ciblées, notamment les chevaux de Troie, les dangers liés au chat, à la création de « homepages » ou encore au blogging. Pour finir, les contre-mesures appropriées sont exposées et expliquées. Citons notamment les contre-mesures humaines comme la vigilance, la méfiance et le savoir-faire, ainsi que les contre-mesures techniques comme la restriction de fonctionnalités non utilisées et la mise à jour du système d'exploitation, l'antivirus et le firewall.

S'ajoute à cette présentation une séance de sensibilisation expliquant aux jeunes pourquoi ils ne doivent pas s'engager dans la voie du piratage informatique ou du harcèlement (cyberbullying).

A la lumière des informations issues des faits rapportés ou encore des réactions provoquées lors de ces présentations, ce rapport dresse un état des lieux de la situation actuelle.

L'e-inclusion et ses conséquences

On constate que presque la totalité des adolescents et enfants rencontrés a un ordinateur à son domicile ainsi qu'un accès à Internet. Parmi ceux-ci, nombreux sont ceux dont l'ordinateur se trouve dans leur propre chambre à coucher (chiffre estimé à 10-20%). Ils peuvent, ainsi, surfer sur Internet et jouer sans aucune surveillance. Le film de sensibilisation « Wo ist Klaus » montre les éventuelles conséquences de l'utilisation de ces technologies sans l'accompagnement et les conseils d'un adulte.

Les enfants utilisent leurs ordinateurs à des fins multiples. La majorité s'en sert pour surfer, pour communiquer dans des réseaux chat ou encore pour gérer leur page web personnelle.

On remarque que les jeunes ont une forte inclination vers la communication via le chat plutôt que via les courriers électroniques. En général, la communication électronique ne se fait qu'avec un nombre de camarades assez restreint. Les chat rooms publics ne sont pas aussi souvent utilisés que les chats via, par exemple, MSN ou ICQ. Beaucoup utilisent conjointement la webcam (chiffre estimé à 30%) et le micro pour chatter.

Les pages web gérées par les enfants servent de « cartes de visite ». Elles leur permettent de faire leur propre « marketing » ou encore de tenir des sites de photos pour que leurs proches résidant à l'étranger puissent suivre leur vie familiale au Luxembourg. Ainsi, nous avons rencontré des enfants même très jeunes (8 ans) qui gèrent des sites de photos familiales. Ils mettent des images en ligne sans savoir que celles-ci ne sont pas protégées contre la copie.

Beaucoup d'adolescents téléchargent des fichiers mp3 ou des vidéos, installent des jeux téléchargés sans se soucier de leur provenance ou de leur contenu réel (chevaux de Troie ou encore spyware). Certains visitent même des sites de type cracking pour récupérer des générateurs de clés ou des crackers de mots de passe, sans pour autant savoir ce qu'ils risquent sur ces sites (voir la cartographie du malweb¹). D'autres téléchargent des outils d'attaque (chiffre estimé à 2-3%) et certains savent même comment changer leur adresse IP toutes les trente minutes pour ne pas être repérés.

Les adolescents et même les enfants utilisent les mêmes applications et services web que les adultes, à l'exception de l'e-banking. Ils ont aussi des identités électroniques, confient beaucoup de données très personnelles à leur ordinateur et ne se soucient pas vraiment des dangers liés à l'utilisation de l'Internet. Ils ne sont ni conscients de la valeur des données qu'ils confient à un ordinateur non sécurisé, ni de l'ampleur des risques auxquels ils s'exposent par leur négligence et leur bas niveau de savoir-faire.

La majorité a déjà été confrontée à des virus sur leur ordinateur. Pourtant, ils ont tendance à ignorer ou à accepter l'existence de virus sur les ordinateurs, faute de savoir-faire pour les éviter, les trouver et les éradiquer.

¹ <http://www.cases.public.lu/fr/risques/2007/malweb/index.html>

Quasiment tous les enfants et adolescents ont un téléphone mobile dont la plupart sont équipés de caméras et de la fonctionnalité bluetooth. Beaucoup accèdent même à Internet avec leurs téléphones mobiles. L'utilisation de MMS est aussi assez répandue.

L'utilisation excessive de ces moyens de communication, et notamment, dans le cadre de plus en plus répandu du harcèlement, a mené beaucoup d'établissements scolaires à interdire l'utilisation de téléphones mobiles dans l'enceinte des écoles.

Analyse des expériences rapportées

MOTS DE PASSE

Les enfants et adolescents gèrent plusieurs outils de communication² ou services en ligne³ dont l'accès repose sur un identifiant et un mot de passe. Nombreux sont les jeunes qui ne discernent pas l'importance de ces codes d'accès. Ils n'ont même jamais pensé aux conséquences que pourrait avoir une divulgation de leurs données personnelles ou à ce qu'un attaquant pourrait faire s'il connaissait leur identifiant et leur mot de passe à des services en ligne.

Beaucoup de jeunes choisissent des mots de passe très faciles à deviner ou, parfois, partagent même leur mot de passe avec leurs camarades. Ces imprudences de la part des jeunes peuvent avoir des conséquences très fâcheuses telles que la défiguration de sites Internet, la perte de confidentialité des courriers électroniques, la perte de réputation due à des injures ou des propos désobligeants faites en leur nom dans des forums ou des chats. Ces cas ont été fréquemment relatés par les jeunes lors des présentations.

La plupart des jeunes ne connaissent pas les techniques existantes pour récupérer les mots de passe comme l'attaque par dictionnaire, l'attaque ciblée par le social engineering, le « shoulder surfing » ou encore des programmes tels que les keyloggers ou chevaux de Troie.

La naïveté sur laquelle repose ce problème est directement imputable à l'âge des jeunes. Ce n'est qu'à partir de 14-15 ans qu'ils commencent à se rendre compte de certains dangers, c'est-à-dire après sept ans d'utilisation d'Internet.

MALWARES

Presque tous les enfants et jeunes savent qu'il y a des virus. A contrario, peu connaissent l'existence des vers et ce qui les différencie des virus. Quasiment personne ne peut associer un concept aux malwares. Le nombre de jeunes tend vers zéro lorsqu'il s'agit de définir comment fonctionnent ces malwares, et plus précisément, quelles vulnérabilités

² Ordinateur, GSM

³ MSN, e-mail, homepage, blogg, jeux en ligne, forums, etc.

ces malwares exploitent. Nettement plus de la moitié ont déjà subi les conséquences d'infections de vers ou de virus. Celles-ci sont souvent perçues comme une « fatalité » à laquelle on ne peut échapper. Les jeunes considèrent que la destruction des fichiers qui se trouvent sur leur ordinateur est l'impact maximal d'une telle infection. Cependant, ils ne prennent que trop rarement en considération les conséquences découlant d'une perte de confidentialité, d'intégrité et du vol d'identité.

Ce comportement « fataliste » peut, bien sûr, avoir des retombées catastrophiques, particulièrement en cas d'infection par un cheval de Troie, un malware conçu pour espionner discrètement et non pour détruire. Une infection par un cheval de Troie ne se détecte pas aussi rapidement que celle par un ver destructeur. Surtout si on pense que dans beaucoup de foyers, tous utilisent un même ordinateur familial et que tous ont des droits d'administrateur qu'ils lèguent aux malwares qu'ils attrapent.

Quelques cas nous ont été rapportés où des jeunes utilisent des chevaux de Troie pour espionner leurs camarades, par exemple, pour contrôler leur webcam et pour lancer des vrais espionnages à l'insu de la victime. À l'exception de la classe d'une victime d'un tel espionnage, les jeunes n'étaient pas conscients de ce risque et étaient stupéfaits d'apprendre qu'il est possible de les espionner de la sorte.

Les vecteurs d'infection les plus répandus sont le téléchargement via Internet de fichiers infectés, la visite de sites appartenant au malweb⁴, le fait d'accepter des fichiers depuis MSN ou des forums de chat. Comme nous l'avons vu, le courrier électronique n'est pas autant utilisé et, de ce fait, n'est pas un vecteur d'infection fréquent.

CHAT

L'utilisation du chat est très populaire parmi les jeunes. Dès l'école primaire, MSN est l'outil le plus utilisé. L'avantage de cet outil est la possibilité de ne chatter qu'avec des personnes invitées (white listing). En avançant dans l'âge, les jeunes commencent à fréquenter des forums en ligne.

L'utilisation excessive de MSN amène parfois des parents à interdire son utilisation, ce qui pousse les enfants vers des forums ouverts et non limité à leurs pairs.

L'usurpation de mots de passe est un problème que beaucoup de jeunes ont déjà rencontré. Celui-ci est lié soit au choix d'un mauvais mot de passe, soit au partage de mots de passe entre camarades.

Dans les forums de chat, les injures, diffamations et calomnies ne sont légion. A cela s'ajoute un langage assez cru, particulièrement dans des forums ouverts. En outre, beaucoup de jeunes n'ont pas conscience que le choix de leur pseudonyme peut leur attirer des problèmes⁵.

⁴ Infection par un trojan downloaders directement ou via iFrame

⁵ Lolita13, aimée12, bunny14

Les programmes de chat comme MSN sont employés comme canaux de distribution des malwares, notamment les chevaux de Troie. Certains jeunes n'ont aucun scrupule à utiliser ces programmes pour espionner, brancher des caméras (webcam) ou prendre le contrôle des téléphones portables de leurs camarades.

Les jeunes sont conscients qu'ils doivent être prudents dans les chat rooms. Ils savent qu'ils ne doivent révéler ni leur vrai nom, ni leur adresse, ni leur numéro de téléphone. Toutefois, certains cas ont été relevés où des jeunes avaient physiquement rencontré des personnes qu'ils ne connaissaient que via Internet, et ce, en toute connaissance de cause. Les raisons invoquées restent floues. Certains disent qu'ils sont « tombés amoureux » et d'autres qu'ils voulaient rencontrer la personne « par curiosité ».

Parfois, ils rencontrent aussi des personnes qu'ils ne connaissent que par l'intermédiaire des forums de chat pour réaliser des achats ou des ventes. On peut citer le cas d'un élève d'une école primaire fixant un rendez-vous à un « enfant » afin de « finaliser » une vente entamée sur Internet...mais, lors du rendez-vous, il s'est retrouvé face à un adulte et non pas face à un enfant de son âge !

Un autre cas nous a été reporté où une adolescente, pour se venger de ses camarades de classe, a inventé un personnage mâle fictif et a commencé à chatter avec ses camarades sous l'identité de ce personnage fictif. Elle a su nouer des liaisons affectives vers certaines camarades de classe. Après avoir soutenu son personnage fictif pendant plusieurs mois, elle a, dans le chat, annoncé que le personnage fictif allait se suicider. Sur cette déclaration, beaucoup de jeunes filles de la classe étaient profondément touchées et choquées et ont eu besoin de support psychologique.

Le harcèlement sexuel de filles de tout âge dans le chat est quelque chose qui nous est rapporté très souvent. Les harceleurs essayent de leur envoyer des images pornographiques, respectivement les incitent à faire des images d'eux-mêmes ou de prendre contact physique avec eux. Vu que beaucoup d'enfants chattent avec comme pseudonyme une adresse de courrier électronique, beaucoup de ces enfants reçoivent aussi des courriers électroniques harcelants. La gêne des enfants leur interdit souvent de parler de ces événements à un adulte. Ces enfants souffrent très souvent seuls et essayent seuls de résoudre le problème. Lors que des parents sont informés, ceux-ci réagissent généralement de façon incorrecte et interdisent l'utilisation du chat ou punissent même l'enfant victime. Lors des cours les enfants ne se sont généralement adressés qu'à nos formatrices plutôt qu'aux formateurs. Les enfants ne s'ouvrent que si on adresse directement le problème du harcèlement sexuel.

INTERNET

Très rares sont les jeunes - enfants et adolescents - qui n'ont pas encore surfé sur Internet. La plupart utilise Internet sans l'assistance d'un adulte. Inconscients des dangers, insouciantes et naïfs, les jeunes visitent tous les sites et téléchargent quantité de fichiers sans se soucier des éventuels dangers.

Beaucoup (entre 10 % et 20% des lycéens) nous ont rapporté être devenus eux-mêmes victimes d'escroqueries liées à des abonnements. Ces cas s'aggravent si les enfants en questions n'osent pas en parler à leurs parents par crainte des punitions.

La fréquentation de sites pornographiques cause aussi des soucis à certains jeunes. En effet, ces visites sont suivies d'envois de spams qui polluent leur boîte mail et ont peur de punitions sévères de la part de leurs parents.

Internet est aussi un moyen pour certains jeunes de se procurer des jeux qui ne sont pas destinés à leur catégorie d'âge. Ainsi, ils peuvent télécharger des jeux qui sont interdits à la vente se trouvent sur l'index et ne sont pas vendus ou qui sont vendus uniquement aux adultes.

Des problèmes liés à la consommation de vidéos violentes voire extrêmement violentes nous ont aussi été signalés par des enfants d'écoles primaires.

HOME PAGE ET SOCIAL NETWORKING

Nombreux sont les jeunes qui réalisent des sites web ou qui se présentent sur des plateformes comme Hi5⁶ ou Facebook⁷. Déjà, à l'école primaire, beaucoup d'enfants débutent leur projet de site web (environ un quart des enfants). Ces sites regorgent de marques protégées, d'images et de fichiers mp3. Les jeunes utilisent ces sites pour se faire leur propre publicité.

Certains, particulièrement les enfants de familles immigrées, utilisent Internet pour rester en contact avec les membres de leur famille restée dans leur pays d'origine.

Peu sont conscients du fait que chaque internaute peut consulter leur page web. Ils confondent le Word Wide Web avec le « white listing » de MSN.

Tous sont inconscients des lois touchant aux marques et aux œuvres d'art. Ils ne comprennent pas pourquoi ils devraient demander l'autorisation des personnes concernées avant de publier des photos sur Internet. Il y a même des jeunes qui publient des détails très privés ou publient des photos lascives sans se rendre compte des conséquences d'un tel acte. En outre, beaucoup croient qu'il est possible de protéger les images ou photos de leur site contre la copie.

Malheureusement, Internet est aussi assez souvent utilisé afin de propager des diffamations et des calomnies. Les jeunes ne connaissent pas les lois qui protègent leur droit à la vie privée et ne se fient pas aux adultes ou à la police pour faire cesser ces agissements.

⁶ <http://www.hi5.com/>

⁷ <http://www.facebook.com/>

TELEPHONES MOBILES

Quasiment tous les enfants (généralement à partir de la première communion) ont déjà un téléphone mobile. Ces téléphones sont généralement équipés, en plus des fonctionnalités voix, d'un appareil photo, d'écrans couleurs, d'une connectivité vers Internet (GPRS, WiFi), de Bluetooth, MMS, SMS, de capacités plus ou moins grandes afin de stocker des fichiers mp3, photos et vidéos.

Les jeunes se servent de leurs téléphones mobiles pour communiquer entre camarades et pour organiser leur vie privée. Seulement, beaucoup les utilisent aussi pour toutes formes inimaginables de harcèlement. A titre d'exemple, citons la prise de photos dans des salles de classe ou les vestiaires qui a mené beaucoup d'écoles à interdire l'utilisation de téléphones mobiles dans l'enceinte des établissements.

Le partage de films extrêmement violents (happy slapping, snuff, exécutions, etc.) ou à contenus pornographiques est à la mode, même parmi les enfants des écoles primaires. Certains enfants rapportent qu'ils en souffrent. Dans certains cas, les enfants ou adolescents ont même été forcés de regarder ces films extrêmement violents ou à les stocker sur leur téléphone portable.

L'utilisation de « super bluetooth », application java tournant sur les téléphones mobiles destinée à prendre le contrôle d'autres appareils munis de bluetooth, se répand très vite d'un lycée à l'autre. Cet outil d'attaque est très efficace et peut causer des dommages conséquents en cas de compromission d'outils de plus en plus performants disposant d'informations hautement confidentielles et personnelles.

Analyse des compétences

Les jeunes et enfants adoptent facilement les nouvelles technologies, et particulièrement celles employées pour communiquer se présentant sous forme d'accessoires ou d'applications à prix modique ou même gratuits et qui leur permettent de faire leur propre « promotion »

On constate de faibles compétences techniques. Au-delà de l'utilisation de ces accessoires et applications, leur fonctionnement leur est totalement méconnu. En outre, très rares sont ceux qui cherchent à en comprendre la technologie.

Ils ne connaissent pas les dangers du web et visitent les sites qui offrent ou promettent des contenus gratuits susceptibles de les intéresser. Beaucoup téléchargent des petits jeux ou des applications sans se soucier du malware qui pourrait s'y dissimuler.

Les jeunes ne savent pas qu'Internet est un gigantesque réseau informatique qui connecte plusieurs centaines de millions de personnes. Ils n'ont pas conscience de l'ampleur du réseau et des différents profils de personnes qui l'utilisent. Leur inconscience, leur manque de méfiance et leur naïveté les rend vulnérables à différents types d'attaques.

Prévention et application de contre-mesures

REPRESSION

Les enfants ne savent pas qu'ils peuvent faire appel à la police s'ils deviennent victimes ou témoins d'une attaque de cyberbullying. Ils ne sont en fait pas conscients que les lois ont été créées pour protéger les citoyens et non pas pour les punir.

Ils doivent apprendre que contacter la police, ce n'est pas « donner » quelqu'un, mais que c'est un acte de défense ou un appel aux secours tout à fait légitime.

MOTS DE PASSE

Les mots de passe choisis par les jeunes sont souvent très faciles à deviner : noms propres ou numéros de téléphone. Le même mot de passe est souvent utilisé pour chaque système, ce qui implique que si quelqu'un trouve un mot de passe, il aura accès à tous les services utilisés par cette personne.

Malheureusement, beaucoup de jeunes confient leurs mots de passe aussi aux navigateurs tels que Internet Explorer ou Firefox et ne se doutent pas des dangers que cela implique.

Souvent, les jeunes ignorent qu'ils doivent sortir des applications web par le bouton « se déconnecter » pour empêcher qu'un tiers (à la bibliothèque ou dans un cybercafé) puisse avoir accès aux applications en restaurant les sessions interrompues.

ANTIVIRUS

Tous les jeunes savent qu'il est important d'avoir un antivirus, mais beaucoup ne savent pas qu'il faut le mettre à jour régulièrement, au moins deux fois par semaine. On rencontre souvent des jeunes qui prétendent avoir un antivirus, mais la licence étant périmée, ils ne reçoivent plus les mises à jour.

Seulement, peu de jeunes savent qu'un citoyen peut avoir accès à des produits gratuits.

Nombreux (plus de la moitié) sont pourtant ceux qui ont déjà subi les conséquences d'une attaque par malware.

FIREWALL

L'utilisation de firewall personnel est très rare. Le concept des firewalls est méconnu de la plupart des jeunes.

PATCH

L'importance des mises à jour est sous-estimée. Beaucoup pensent que ce sont des rappels dont ils ont déjà connaissance. Ils les ferment donc dès qu'ils les voient. Aucun jeune ne connaît la raison pour laquelle il est indispensable de faire les mises à jour et aucun ne sait que ces mises à jour doivent être installées pour toutes les applications se trouvant sur l'ordinateur.

Spyware remover

Peu nombreux sont les jeunes qui utilisent des logiciels de spyware remover.

Conclusion

Les jeunes, enfants et adolescents, adoptent rapidement toutes les nouvelles technologies de l'information et les utilisent à toutes fins utiles. Cependant, leur manque de connaissances et de méfiance les rend vulnérables à beaucoup de dangers issus de la société de l'information. Ainsi, le vol d'identité ou encore le bullying sont des menaces très communes dans le monde des jeunes.

Il est devenu impératif d'accompagner et d'encadrer les enfants et jeunes dans leur découverte des nouvelles technologies, mais il importe aussi d'aider les parents, éducateurs et formateurs de suivre et de comprendre ce mouvement.