



CHAMBRE DES DÉPUTÉS
GRAND-DUCHÉ DE LUXEMBOURG

Session ordinaire 2012-2013

CH/vg

P.V. ENFPS 11
P.V. ERMCE 15

**Commission de l'Education nationale, de la Formation
professionnelle et des Sports**

et

**Commission de l'Enseignement supérieur, de la Recherche, des
Media, des Communications et de l'Espace**

Procès-verbal de la réunion du 31 janvier 2013

Ordre du jour :

1. Echange de vues avec des représentants de BEE SECURE au sujet des activités visant à sensibiliser les jeunes à une utilisation plus sécurisée des nouvelles technologies de l'information et de la communication
2. Pour les membres de la Commission de l'Education nationale et de la Formation professionnelle :

Adoption du projet de procès-verbal de la réunion du 10 janvier 2013

*

Présents : M. Claude Adam, M. André Bauler, M. Eugène Berger, M. Fernand Diederich, M. Emile Eicher, M. Ben Fayot, M. Claude Haagen, M. Fernand Kartheiser, M. Gilles Roth, M. Jean-Paul Schaaf, Mme Tessy Scholtes, membres de la Commission de l'Education nationale, de la Formation professionnelle et des Sports

M. Claude Adam, Mme Diane Adehm, M. Eugène Berger, M. Jean Colombero, Mme Claudia Dall'Agnol, M. Ben Fayot, M. Claude Haagen, M. Marcel Oberweis, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

Mme Mady Delvaux-Stehres, Ministre de l'Education nationale et de la Formation professionnelle

M. François Thill, du Ministère de l'Economie

M. Eric Krier, du Service National de la Jeunesse

M. Daniel Weiler, du Ministère de l'Education nationale et de la Formation professionnelle

M. René Schlechter, Président de l'Ombudscomité fir d'Rechter vum Kand

Mme Christiane Huberty, de l'Administration parlementaire

Excusés : M. Serge Wilmes, membre de la Commission de l'Education nationale, de la Formation professionnelle et des Sports

Mme Anne Brasseur, Mme Christine Doerner, M. Norbert Hauptert, M. Serge Wilmes, membres de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

*

Présidence : M. Ben Fayot, Président de la Commission de l'Education nationale, de la Formation professionnelle et des Sports
M. Marcel Oberweis, Président de la Commission de l'Enseignement supérieur, de la Recherche, des Media, des Communications et de l'Espace

*

1. Echange de vues avec des représentants de BEE SECURE au sujet des activités visant à sensibiliser les jeunes à une utilisation plus sécurisée des nouvelles technologies de l'information et de la communication

En introduction, M. le Président de la Commission de l'Education nationale, de la Formation professionnelle et des Sports précise que c'est suite à l'incitation de M. le Président de la Chambre des Députés que les deux Commissions réunies ont pris l'initiative de s'intéresser de plus près aux activités proposées pour sensibiliser les jeunes à une utilisation plus sécurisée des nouvelles technologies de l'information et de la communication (ci-après : TIC).

A préciser d'emblée que BEE SECURE est une initiative commune du Ministère de l'Economie et du Commerce extérieur, du Ministère de la Famille et de l'Intégration et du Ministère de l'Education nationale et de la Formation professionnelle. Ce projet est aussi financé en partie par la Commission européenne, et fait fonction de centre de sensibilisation luxembourgeois au sein du réseau paneuropéen Insafe.

Notons encore qu'en amont de la présente réunion, les membres des deux Commissions se sont vu mettre à disposition une importante documentation reprenant des échantillons du matériel utilisé par BEE SECURE dans le cadre de ses activités de sensibilisation.

• **Présentation de BEE SECURE**

A l'aide d'un document *PowerPoint*, les experts retracent les origines de l'initiative BEE SECURE, présentent leur approche et les activités offertes, ainsi que les défis auxquels ils se voient actuellement confrontés. A cet effet, il est renvoyé à la présentation reprise à l'annexe 1 du présent procès-verbal.

En dehors des informations fournies par la présentation même, retenons succinctement les éléments suivants :

- Historique (p. 4)

Alors que CASES Luxembourg (Cyberworld Awareness & Security Enhancement Services) a été créé dès 2003, c'est en 2008 qu'a été signé un « memorandum of understanding » entre le Ministère de l'Education nationale et de la Formation professionnelle, le Ministère de la

Famille et de l'Intégration, ainsi que le Ministère de l'Economie et du Commerce extérieur, en vue de coordonner l'approche gouvernementale en matière de sensibilisation du grand public, et notamment des enfants et des jeunes, à une utilisation plus sécurisée des nouvelles technologies de l'information et de la communication. C'est à ce moment qu'a été introduite une formation *ad hoc* obligatoire dans les classes de 7^e de l'enseignement secondaire et secondaire technique. Il s'est révélé entre-temps que cette formation intervient relativement tard dans le développement des jeunes, étant donné que la majorité d'entre eux ont déjà fait bon nombre d'expériences auparavant dans le domaine des TIC. Il s'agit en quelque sorte du tout dernier moment où il est encore possible de protéger les jeunes face à certains risques liés à l'utilisation des TIC et d'éviter que de mauvaises habitudes s'enracinent.

Dans cette optique, depuis 2011, les formations sont étendues au cycle 4, et même au cycle 3, de l'enseignement fondamental. De fait, le cycle 3.1. représente un moment crucial en matière de prévention, dans la mesure où, dans le cadre de la première communion, de nombreux enfants se voient offrir toutes sortes d'appareils technologiques.

– Situation actuelle (p. 5)

A l'heure actuelle, BEE SECURE organise 550 formations dans les écoles, touchant quelque 10.000 jeunes. Ces formations se font par classe et sont assurées par des experts externes. Elles permettent à ces derniers de gagner un aperçu unique et approfondi sur les tendances du moment, les problèmes et les soucis auxquels se voient confrontés les jeunes. Depuis quelques années, les connaissances et les expériences ainsi acquises sont rassemblées et synthétisées dans des rapports annuels. Le rapport pour 2012, mis à la disposition des membres des deux Commissions, est repris à l'annexe 2 du présent procès-verbal.

Par contre, le nombre de parents et d'enseignants et éducateurs touchés respectivement par les soirées pour parents d'élèves et les formations laisse encore à désirer.

– Approche (p. 6)

L'approche retenue peut être qualifiée de collaborative, dans la mesure où de nombreux acteurs se retrouvent et se présentent sous le nom de « BEE SECURE » pour contribuer à la sensibilisation du grand public, et notamment des enfants et des jeunes. Financée essentiellement par le Gouvernement luxembourgeois, la marque BEE SECURE constitue un acteur neutre, qui ne dépend pas d'un financement commercial.

– BEE SECURE pour les écoles (p. 7)

Il importe que les différentes formations et actions de sensibilisation soient coordonnées par un acteur, en l'occurrence le Service National de la Jeunesse, pour assurer la cohérence des messages diffusés.

Alors que les formations dans les écoles mettaient dans un premier temps l'accent sur le volet technologique, elles sont centrées, depuis 2010, sur le comportement des enfants et des jeunes et s'articulent autour de plusieurs thèmes (sécurité technique, consommer en ligne, communiquer en ligne, cyber-bullying).

Il est veillé à ce que le nombre des participants soit suffisamment réduit pour permettre une approche interactive.

Comme signalé ci-dessus, les formateurs sont des experts externes qui doivent se prévaloir à la fois de connaissances approfondies en matière de TIC et de compétences pédagogiques, étant entendu qu'ils se voient proposer régulièrement des formations continues. Par ailleurs a été mis en place un label pour les formateurs, ce qui contribue à assurer la qualité des formations. L'efficacité de ces dernières est désormais évaluée par l'unité de recherche INSIDE (Integrative Research Unit : Social and Individual Development) de l'Université du Luxembourg.

– Infrastructures (p. 8)

BEE SECURE propose en outre, via la structure CASES, une analyse des risques de l'équipement technologique de certaines infrastructures telles que les maisons de jeunes, les écoles fondamentales et les lycées. Suite à une telle évaluation, les acteurs de BEE SECURE émettent des recommandations en termes de politique de sécurité et proposent, le cas échéant, des solutions en vue de l'implémentation de mesures de sécurité.

Un défi actuel est posé par la pratique de plus en plus répandue d'utiliser le même équipement technologique à la fois à des fins privées et professionnelles (« bring your own device »). En résultent en effet de nouveaux risques en matière de sécurité de l'information.

– BEE SECURE pour les parents et encadrants (p. 9)

La page 9 de la présentation fournit un aperçu sur les initiatives de BEE SECURE pour sensibiliser les parents et les enseignants à la problématique. A côté des formations proprement dites, BEE SECURE propose aussi du matériel didactique destiné aux différents groupes-cibles.

En ce qui concerne les parents et les grands-parents, il s'agit de transmettre le message que, face au constat selon lequel l'approche des jeunes en matière de TIC se distingue considérablement de leur propre pratique, il importe avant tout de suivre les activités de leurs enfants dans ce domaine et de ne pas négliger le dialogue intergénérationnel.

Quant aux enseignants, ils se voient proposer des activités qu'ils peuvent intégrer dans leurs cours, en vue de pérenniser les messages transmis lors des interventions assurées par BEE SECURE et de faire ainsi figure de multiplicateurs.

Le défi consiste dès lors à atteindre un nombre plus important des acteurs susmentionnés. Une des pistes possibles est de proposer en 2013 des cours de type « Lunch and learn », qui permettront à des parents de se former pendant la pause de midi. Pour ce qui est du personnel enseignant et éducatif, il serait opportun que BEE SECURE puisse intervenir dans les formations initiales des enseignants et éducateurs. De même, il faudrait encore élargir l'offre dans le cadre de la formation continue.

– Campagnes (p. 10)

La page 10 de la présentation est consacrée aux campagnes lancées par la marque BEE SECURE qui regroupe à cet effet de nombreux partenaires. En termes d'approche, il importe de situer les différentes campagnes dans le contexte général de la culture de la sécurité. C'est ainsi que BEE SECURE peut contribuer à la formation de futurs adultes qui ne disposent pas seulement de solides compétences technologiques mais qui aient aussi intériorisé les principes de sécurité de l'information.

Signalons que la campagne 2013-2014 de BEE SECURE sera dédiée au sujet de la cyberdépendance. Il convient en effet d'établir la distinction entre un comportement « sain » en matière de TIC et un comportement addictif.

– Défis à court terme (p. 11)

A la page 11 de la présentation sont énumérés les défis auxquels se voit confronté BEE SECURE à court terme.

A noter que, compte tenu du fait que c'est à un âge de plus en plus jeune que les enfants ont leurs premiers contacts avec les TIC, il est prévu d'élaborer du matériel visant le niveau de l'éducation précoce.

• **Echange de vues**

De l'échange de vues subséquent, il y a lieu de retenir succinctement les éléments suivants :

- Selon le rapport 2012 de BEE SECURE, les jeunes utilisent leur PC en moyenne deux heures par jour, et pendant les fins de semaine même environ quatre heures par jour. S'y ajoute la consommation d'autres médias (cf. télévision, écoute de musique, etc.).

BEE SECURE n'a pas réalisé d'étude permettant de mesurer l'impact de ce comportement sur les résultats scolaires. Même si de nombreuses études étrangères font état des difficultés croissantes des jeunes à se concentrer durablement sur une tâche donnée, l'on ne peut pas affirmer que ce comportement entraîne d'office des conséquences négatives sur le plan scolaire. Ainsi, il ne faut pas perdre de vue que les TIC peuvent aussi être utilisées avec profit dans le cadre des devoirs à domicile, que ce soit pour rechercher des informations ou pour s'échanger avec des camarades de classe sur une matière donnée. De fait, les pratiques informatiques des jeunes se caractérisent par une intrication intime entre les domaines des loisirs et des études, si bien que l'on peut s'interroger sur l'utilité et l'efficacité de mesures pédagogiques visant à imposer aux jeunes des restrictions en matière d'utilisation des outils technologiques.

Par contre, il est évident qu'un comportement addictif, qualifié de « cyber-dépendance », ne manque pas d'avoir des répercussions négatives sur les résultats scolaires. L'on peut aussi penser dans ce contexte à l'addiction à certains jeux électroniques. Dans ces cas, il ne s'agit pas de simples pratiques qui risquent d'être la source de distractions et de rendre plus difficile la concentration, mais d'un comportement obsessionnel qui fait en sorte que la personne atteinte évolue dans un monde virtuel. Nous avons noté ci-dessus que la prochaine campagne de BEE SECURE sera justement consacrée à cette problématique.

Mme la Ministre confirme que l'omniprésence des TIC change en profondeur le processus d'apprentissage, dans la mesure où les jeunes ont désormais une tout autre approche en ce qui concerne par exemple la recherche d'informations ou la communication. Il en résulte un défi considérable pour l'Ecole, d'autant qu'il est établi que le succès scolaire est encore et toujours largement tributaire des compétences de lecture et du goût de la lecture des jeunes.

- Il ressort du rapport 2012 de BEE SECURE que bon nombre d'enfants de dix ans possèdent déjà un compte auprès de « Facebook », alors que la limite d'âge officielle est fixée à 13 ans. Or il n'existe aucun moyen de contrôle dans ce domaine.

- L'on peut présumer qu'environ 30% des enfants sont à un moment donné victimes d'une forme quelconque de harcèlement en ligne (« cybermobbing »), étant entendu que la durée et la gravité des faits varient selon les cas.

En tout état de cause, le « cybermobbing » a un impact plus destructeur et durable que d'autres formes de harcèlement moral. De fait, il n'existe aucune protection efficace face à ce phénomène et aucun moyen de s'y soustraire. Une fois qu'une donnée figure en ligne, elle y est en quelque sorte pérennisée. Dans cette optique, l'on peut considérer qu'une action ponctuelle lancée via Internet peut avoir un impact comparable à celui de dix ans de harcèlement moral.

- Les pratiques précitées soulèvent inévitablement la question de la répression des abus. Est-il indiqué de priver un enfant de ses appareils électroniques afin de le punir d'un quelconque abus ?

Les représentants de BEE SECURE donnent à penser qu'une démarche purement répressive risque de détruire toute relation de confiance intergénérationnelle. Il se peut alors que les enfants refusent désormais toute communication avec les adultes au sujet de leurs activités en ligne. Les experts prônent plutôt une démarche fondée sur la prévention, la protection et l'aide suite à un incident.

Dans la même veine émerge la question de savoir s'il est encore opportun d'interdire l'usage du téléphone mobile à l'école.

Les représentants de BEE SECURE font valoir que si les jeunes sont à un moment donné privés de l'usage de leur portable, ils ont tendance à s'adonner par la suite à une consommation d'autant plus importante, dans la mesure où il existe un réel besoin de communication qui doit dès lors être « rattrapé ».

Plutôt que de miser simplement sur l'interdiction et la répression, il serait indiqué d'émettre aussi des messages positifs et de valoriser les effets positifs des TIC (cf. mise en réseau des jeunes, recherche d'informations, etc.). Dans cette optique, il serait concevable pour les enseignants de prévoir, à un moment donné de leur cours, des activités, par exemple des travaux de recherche, pour lesquels peuvent être utilisés les téléphones mobiles de type « smartphone ». Une fois que cette activité est terminée, les élèves peuvent être invités à ranger leur appareil et à se concentrer sur la prochaine phase du cours.

Les membres des deux Commissions défendent des positions divergentes en cette matière. Alors que certains considèrent que l'usage du portable pendant les cours, et en dehors des activités décrites ci-dessus, est problématique et que les élèves sont tout à fait disposés à accepter des règles claires à ce sujet, d'autres estiment que les jeunes sont de nos jours capables de suivre un cours, tout en utilisant de temps en temps leur « smartphone ».

- Les formations proposées par BEE SECURE dans les écoles rencontrent en général un écho très favorable. Le fait qu'elles sont assurées par un intervenant externe contribue à en renforcer l'efficacité. Comme l'enseignant assiste toutefois à la formation, il a l'occasion de gagner un aperçu approfondi sur les pratiques informatiques de ses élèves et dispose ainsi d'une matière de discussion sur laquelle il lui est loisible de revenir à l'occasion. Il peut en effet s'avérer utile d'approfondir par la suite certains sujets, dans la mesure où la durée de la formation de BEE SECURE est forcément limitée dans le temps.

Il semble évident que le message peut être transmis avec d'autant plus de succès si les mauvaises habitudes ne sont pas déjà ancrées auprès des jeunes. Voilà pourquoi les représentants de BEE SECURE estiment qu'il serait indiqué de vérifier l'opportunité d'avancer le moment de la formation obligatoire.

En termes d'évaluation, les élèves et les enseignants se voient soumettre un questionnaire à l'issue de la formation. Il en ressort que plus de trois quarts des élèves se montrent satisfaits de la formation. Plus de 90% des enseignants émettent aussi un avis positif et se déclarent convaincus de la plus-value de cette formation.

- Il est constaté qu'il serait important de prévoir dans les formations initiales des enseignants des modules consacrés à l'éducation aux médias et à la sensibilisation des futurs enseignants aux multiples défis qui se posent dans ce domaine. Dans ce contexte est rappelée la motion votée le 8 juin 2010 par la Chambre des Députés et invitant le Gouvernement « à étendre l'éducation aux médias à tous les niveaux de l'enseignement fondamental et secondaire ainsi qu'à l'accueil éducatif des enfants et des jeunes dans les maisons relais et les maisons des jeunes ».

Quant à la formation continue des enseignants, il se pose la question de savoir s'il ne serait pas utile de faire figurer cette matière parmi les domaines de formation obligatoires.

- Les représentants de BEE SECURE confirment qu'il est difficile d'atteindre une proportion importante de parents, alors que ce serait d'une nécessité primordiale qu'ils se penchent sur le sujet.

Parmi les parents qui assistent aux soirées d'information, il s'agit néanmoins de personnes issues de tous les milieux dont certaines ont déjà des connaissances en la matière et d'autres non. Souvent est d'ailleurs organisée une traduction de la formation. Sur demande, les experts dispensent aussi des formations en plusieurs langues.

La question de savoir si l'encadrement que peuvent offrir les parents en matière de TIC varie en fonction du milieu socioculturel n'a jusqu'à présent pas fait l'objet d'une étude systématique. De façon empirique, les représentants de BEE SECURE estiment que ce n'est pas tant le milieu social qui est décisif que l'attitude des parents. Ainsi, il convient plutôt de faire la distinction entre les parents qui reconnaissent leurs lacunes en la matière et qui sont

prêts à s'intéresser au sujet et à accompagner leurs enfants dans ce domaine, d'une part, et les parents qui laissent leurs enfants plutôt seuls face aux TIC, d'autre part.

- Un membre fait observer que certaines brochures mises à disposition par BEE SECURE, telles que le « Leitfaden für Eltern », semblent d'un accès plutôt difficile. Si ces publications constituent sans doute un appoint utile, elles ne sauraient remplacer la communication directe avec les parents.

En réponse, les représentants de BEE SECURE précisent que compte tenu des ressources humaines limitées dont ils disposent, ils ont en partie recours à du matériel mis à disposition dans le cadre du réseau paneuropéen Insafe auquel appartient BEE SECURE.

- Il est souligné l'importance de favoriser le dialogue intergénérationnel sur les problèmes et les risques liés à l'utilisation des TIC. Souvent, les parents et les enseignants hésitent à aborder le sujet, parce qu'ils craignent de ne pas disposer de suffisamment de connaissances technologiques pour dialoguer avec les jeunes. Or, à y regarder de près, l'on constate que le problème ne réside pas dans ce domaine, d'autant que les connaissances technologiques proprement dites de bon nombre de jeunes sont aussi plutôt rudimentaires. Il importe plutôt de s'échanger sur les problèmes liés à l'utilisation des TIC.

En relation avec le dialogue intergénérationnel, il est soulevé la question de savoir si BEE SECURE ne propose pas d'activités de sensibilisation qui réunissent les différents acteurs concernés, c'est-à-dire les jeunes, les parents et les enseignants.

Les experts répondent qu'il peut arriver que des parents assistent avec leurs enfants aux soirées d'information destinées aux parents, ce qui permet en effet de favoriser le dialogue intergénérationnel. Malheureusement, de tels cas restent encore l'exception.

La volonté de favoriser le dialogue intergénérationnel figure toutefois parmi les défis à court terme identifiés par BEE SECURE (cf. p. 11 de la présentation), et il est tout à fait concevable de développer des produits afférents.

- Suite à un questionnaire y relatif, les représentants de BEE SECURE estiment que la législation luxembourgeoise en matière de protection des données et de sécurité de l'information est assez complète. Ainsi, la loi modifiée du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel, qui a institué la Commission nationale pour la protection des données, mise sur des approches résolument modernes telles que l'analyse des risques.

Le problème consiste toutefois dans le fait que cette législation est peu connue et difficile à comprendre pour le public.

- Les représentants de BEE SECURE attirent encore l'attention sur le « Safer Internet Day 2013 » qui aura lieu le 5 février 2013 et dont le programme peut être consulté à l'adresse suivante : <https://www.bee-secure.lu/fr/saferinternetday>.

M. le Président de la Commission de l'Education nationale, de la Formation professionnelle et des Sports remercie les représentants de BEE SECURE de leur engagement et de l'échange de vues instructif.

2. Pour les membres de la Commission de l'Education nationale et de la Formation professionnelle :
Adoption du projet de procès-verbal de la réunion du 10 janvier 2013

Le projet de procès-verbal susmentionné est adopté.

Luxembourg, le 7 février 2013

La Secrétaire,
Christiane Huberty

Le Président de la Commission de
l'Education nationale, de la Formation
professionnelle et des Sports,
Ben Fayot

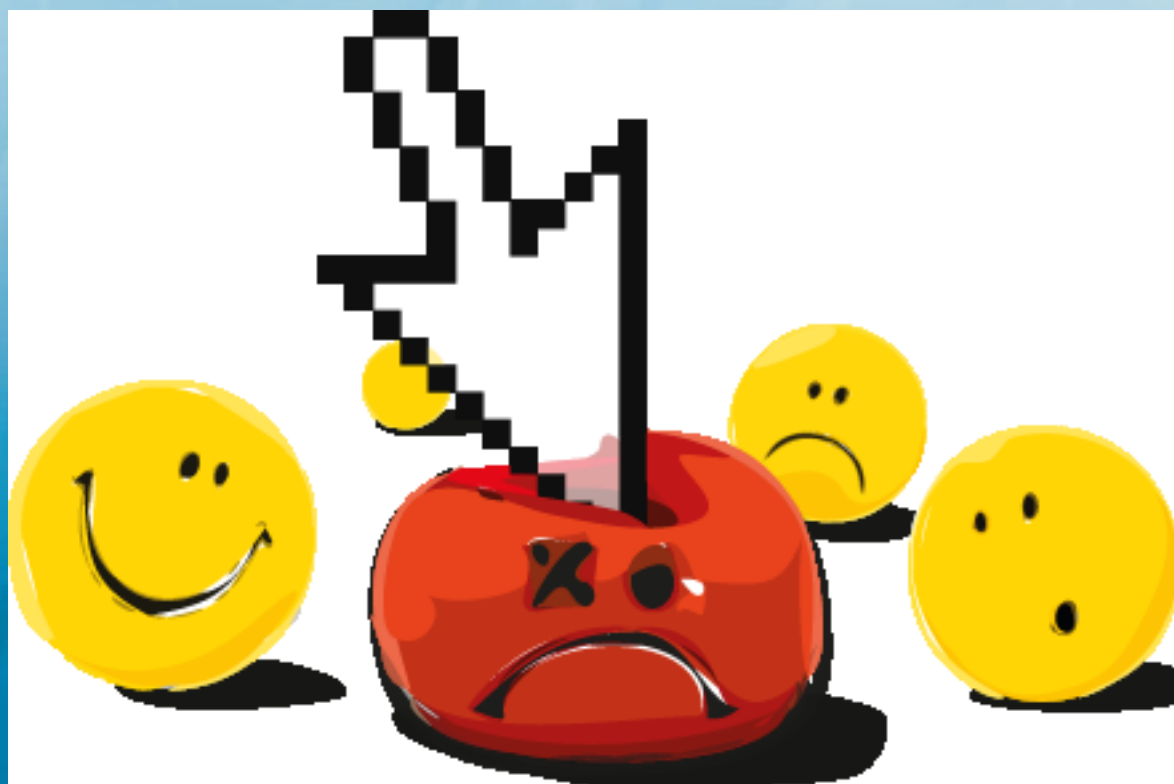
Le Président de la Commission de
l'Enseignement supérieur, de la Recherche,
des Media, des Communications et de
l'Espace,
Marcel Oberweis

Annexes :

1. Présentation *PowerPoint* BEE SECURE
2. *BEE SECURE Schulungen für einen sicheren Umgang mit Computer und Internet – Erfahrungsbericht für das Jahr 2012*

NOT FUNNY
BEE FAIR

BEE
SECURE



**SECURITY
MADE IN
LETZEBUERG**



BEE SECURE @ Chambre des députés

Luxemburg, 31.01.2013

François Thill, Ministère de l'Economie et du Commerce extérieur

Eric Krier, Service National de la Jeunesse

Daniel Weiler, Ministère de l'Education nationale et de la Formation professionnelle

René Schlechter, Ombudsmann fir d'Rechter vum Kand (ORK)

Agenda



- ▶ Historique
- ▶ Approche
- ▶ BEE SECURE pour les écoles
- ▶ Campagnes
- ▶ BEE SECURE pour les parents et encadrants

Historique



- ▶ 2003 création de CASES
- ▶ 2005 première formation lors du “Safer Internet Day” dans le LGL
- ▶ 2008 MOU MinEduc, MinFam, MinEco sur approche gouvernementale pour la sensibilisation du grand public, avec un focus spécial sur enfants et jeunes
- ▶ 2008 première formation “obligatoire” à Wiltz
- ▶ Depuis 2008: couverture +/- 96% des classes de 7^{ième}
- ▶ 2010 lancement de BEE SECURE
- ▶ Depuis 2011: couverture +/- 30% des classes Cycle 4

Situation actuelle



- ▶ 550 formations dans les écoles touchant 10.000 jeunes
- ▶ 30 workshop dans le secteur jeunesse (para-scolaire) touchant 250 jeunes
- ▶ 33 soirées parents d'élèves touchant 300 parents
- ▶ 11 formations pour multiplicateurs touchant 200 enseignants et éducateurs
- ▶ 18 événements jeunes (RAF, On Stéitsch, FFYS, ...)
- ▶ 15 événements grand public (12.000 personnes)



Approche



- Marque commune forte
- Services clients de qualité
- Responsabilités et compétences au niveau opérationnel
- Soutien actif des ministères
- Co-financement / réseaux



Funded by the
European Union



BEE SECURE pour les écoles



- ▶ Focus sur les technologies en 2008
- ▶ Focus sur le comportement depuis 2010, modularisation des thèmes
- ▶ Thèmes:
 - ▶▶ Sécurité technique (20 min)
 - ▶▶ Consommer en ligne (10 min)
 - ▶▶ Communiquer en ligne (40 min)
 - ▶▶ Cyber-bullying (15 min)
- ▶ Interactif grâce au nombre de participants
- ▶ Développement de la qualité
 - ▶▶ Intervenant expert externe
 - ▶▶ Label des formateurs (15 formateurs hommes et femmes!)
 - ▶▶ Évaluation externe de l'efficacité (par INSIDE de UNI.lu)
 - ▶▶ Formation continue (5 fois par an) pour formateurs



Les infrastructures



► Résultats

- Maisons de jeunes (2008)
Écoles primaires (2010) et
Lycées (2010)
 - Analyse des risques et politique de sécurité
 - Implémentation des mesures de sécurité
- Secteur privé – création d'outils



► Défis

- BYOD (« bring your own device »)

BEE SECURE pour les parents et encadrants



- **Contenus**
 - Internet (web 1.0 et web 2.0)
 - Besoins des jeunes
 - Contenus illicites, illégaux et dangereux
 - Compétences médias
 - Communication (chat, webcam, facebook,...)
 - Propriété intellectuelle et droits d'auteurs
- **Supports**
 - Leitfaden
 - Kuck mat wat deng Kanner maachen
- **Défis**
 - Formation initiale ET continue des éducateurs et enseignants
 - Toucher plus de parents
 - Nouvelles formules, p.ex: "lunch and learn" dans les entreprises



Les campagnes



- ▶ Approche
 - ▶▶ Messages positifs...
 - ▶▶ Créer une culture de la sécurité (OCDE)
 - ▶▶ Vision globale et holistique
- ▶ Facteurs de succès
 - ▶▶ Qualité, approche marketing, neutralité
 - ▶▶ Maximum de partenaires
- ▶ Thèmes
 - ▶▶ Mots de passe (2010-2011)
 - ▶▶ Safer Internet / Safer Sex (2011-2012)
 - ▶▶ Not funny – BEE FAIR (2012-2013)
 - ▶▶ Cyber-dépendance (2013-2014)



Défis à court terme



- Répéter – répéter – répéter
- Dialogue intergénérationnel
- Utilisateurs (enfants) de plus en plus jeunes
- Responsabilisation et implication des parents!!
- Besoins spécifiques des grands-parents
- Labels de qualité et de sécurité



SECURITY MADE IN LETZEBUERG



www.bee-secure.lu



facebook.com/beesecure



twitter.com/beesecure



youtube.com/beesecureTV



podcast.bee-secure.lu



Helpline: 26 64 05 44

Suivez le Safer Lunch et la Table Ronde en direct via Live Stream sur www.bee-secure.lu

Safer Internet Day 2013
05.02.2013
Connect with respect!

Online rights and responsibilities
Entrée gratuite

13h30 à 14h00
• **Safer Lunch**, Lunch d'initiation à BEE SECURE
• **Maison du Jeune**, 7 rue du Marché aux herbes, Luxembourg
Sujet: **Harcelement en ligne** – ça commence déjà à l'école primaire
Langue: Français / Ouvert aux parents, enseignants et élèves

16h00 à 18h00
• **Concert** pour le lancement du «**Stop Stupeur**»
• **Contre Adresses** (Partage d'adresses)
Ouvert à tous les jeunes

19h30 à 21h00
• **Table Ronde** «**Web sans mensonge** quel est le gain?»
• **BOL, GNP, PARTIBAS**, coin **Bee** Repaire Web-Dame
Sujet: **Droits à l'image**
• **Tom Krieger**, Avocat et président du Conseil National des Programmes
• **Thierry Lefebvre**, Membre effectif de la Commission Nationale pour la protection des données
• **Romy Schmidt**, Ministre de l'éducation nationale et de la formation professionnelle
• **Caroline Mart**, Rédactrice en chef adjointe RTL, journaliste et mère de 2 enfants
• **Georges Knehl**, Psychologue diplômé, BEE SECURE Helpline and Skopline
Présentateur: **Marc Gieitz**
Langue: Luxembourgeois / Ouvert aux parents, enseignants et jeunes

NOT FUNNY
BEE SECURE



BEE SECURE Schulungen

Für einen sichereren Umgang mit Computer und Internet

Erfahrungsbericht für das Jahr 2012

Zusammenfassung

Dieser Bericht zeichnet ein aktuelles Bild der Computer- und Internetnutzung von Kindern und Jugendlichen in Luxemburg. Er basiert auf den Erfahrungen der BEE SECURE Trainer, die im Jahr 2012 380 Sekundar- und 180 Grundschulklassen sowie weitere Institutionen sensibilisiert haben.

Hierzulande haben alle Schüler Zugriff auf das Internet und so gut wie alle besitzen einen eigenen Computer und/oder ein Smartphone. Die Handhabung dieser Geräte erfordert eine große Portion Verantwortungsbewusstsein. Leider lässt sich feststellen, dass Kinder damit oft überfordert sind. Viren werden als unausweichliches Übel hingenommen, Angst vor Datenverlust haben die Wenigsten und illegale Downloads gelten als Kavaliersdelikt. Zwar gibt es in jeder Klasse einen oder zwei Ausnahmeschüler, die gut informiert sind, doch beim Großteil der Schüler fallen eine nicht zu unterschätzende Naivität, eine gefährliche Sorglosigkeit und eine enorme Risikobereitschaft auf.

Bereitwillig werden persönliche Informationen bis hin zu Kontaktdaten auf sozialen Netzwerken veröffentlicht, Bilder werden uneingeschränkt hochgeladen, manipuliert, vervielfältigt und im weltweiten Netz verbreitet. Dabei fallen zwei Komponenten auf, die das Internet für die Jugendlichen zu einem fast schon „überlebenswichtigen“ Tool machen:

1. Die Möglichkeit der Selbstdarstellung: Das Herumexperimentieren mit verschiedenen Identitätskonzepten (cool, sexy, romantisch, stark,...) und das direkte Feedback darauf in Form von Komplimenten und „Likes“ bestärkt die Jugendlichen vor allem in ihrer Selbstfindungsphase.

2. Das Internet als Kommunikationsmittel um rund um die Uhr mit Freunden in Kontakt zu bleiben, zum Kennenlernen von neuen Leuten und zum Flirten „auf Distanz“.

An dieser Herangehensweise wäre an sich nichts auszusetzen, gäbe es nicht so viele Gefahren, die im weltweiten Netz lauern: 16-jährige Jungs, die junge Mädchen um ein Treffen oder freizügige Bilder bitten und sich dann als pädophile Mittvierziger herausstellen, brutale Videos, vielfältige Formen von Cybermobbing, Viren, Trojaner, Daten- und Passwortklau und vieles mehr. Die BEE SECURE Trainer appellieren an die Schüler, einige simple aber wertvolle Ratschläge zu beherzigen, um diesen Gefahren keine Chance zu geben.

BEE SECURE unterstreicht den positiven Nutzen der modernen Informations- und Kommunikationstechnologien. Diese Technologien dürfen aber nicht unreflektiert den Kindern überlassen werden. Genauso wie Kinder lernen, die Straße bei Grün zu überqueren und sich zu vergewissern, dass auch wirklich kein Auto kommt, müssen sie von Anfang an die Grundregeln der sicheren Computernutzung verinnerlichen. Unabhängig von den großen Erfolgen im Bereich der Schüler-Ausbildung und auf Ebene der nationalen Kampagnen gibt es zwei wichtige Baustellen:

- Den Ausbau der Elternarbeit: BEE SECURE unterstützt Eltern in Bezug auf die Internetnutzung ihrer Kinder, damit sie ihrer Aufsichtspflicht besser nachgehen können.
- BEE SECURE setzt sich außerdem für eine gezielte Aus- und Weiterbildung der Fachkräfte (Lehrer/Erzieher) ein.

Nur wer versteht, was die Kinder im Internet antreibt und was sie dort machen, kann potenzielle Gefahren rechtzeitig erkennen und im Notfall ein adäquater Ansprechpartner sein. Medienerziehung sollte zum wesentlichen Bestandteil jeder schulischen und beruflichen Ausbildung werden.

Das Internet entwickelt sich rasend schnell – mit ihm auch seine Gefahren! Prävention und Reaktion sind die Schlüsselwörter der Informationssicherheit. Nur durch flächendeckende Sensibilisierung aller Altersstufen können sie in die Tat umgesetzt werden.

Inhaltsverzeichnis

Rückblick.....	4
Ablauf der Schulung	4
Jugend und Internet: die aktuelle Situation.....	5
Computer.....	5
Mobiles Internet.....	6
Sicherheit.....	7
Schadpogramme.....	7
Schutzmaßnahmen.....	8
Internetnutzung	9
Soziale Netzwerke (Facebook)	9
Chat	11
E-Mail.....	12
Passwörter.....	13
Recht am eigenen Bild.....	14
Urheberrecht.....	14
Cybermobbing	15
Die Rolle der Eltern.....	16
Die Rolle der Lehrer	17
Ausblick	18

Rückblick

Die ersten Präsentationen und Sensibilisierungskampagnen zum Thema Informations- und Computersicherheit gehen in Luxemburg auf das Jahr 2005 zurück, als MySecureIT, ein gemeinsames Programm des Ministeriums für Wirtschafts- und Außenhandel (vertreten durch CASES¹) und des Bildungsministeriums, den sich häufenden Anfragen diverser Schulen nachging. Ziel war es, Kinder und Jugendliche über die Risiken aufzuklären, welche die Internetnutzung mit sich bringt. **Aufgrund ihres einschlagenden Erfolgs hat das Bildungsministerium die Schulungen ab 2008 für alle Septima-Klassen verpflichtend gemacht.** Ein weiterer wichtiger Schritt bestand in der Bereitstellung des dafür notwendigen Budgets. Ab diesem Zeitpunkt liefen die Schulungen nicht mehr unter dem Namen „MySecureIT“, sondern „Luxemburg sicher im Netz“, in Zusammenarbeit mit dem damaligen europäischen Projekt „LUSI – Luxembourg Safer Internet“.

Nachdem die Durchführung 5 Jahre lang in den Händen von CASES lag, wurde 2010 die Koordinierung der Schulungen an den Service National de la Jeunesse (SNJ) übertragen. Unter dem neuen Namen „BEE SECURE“ werden nunmehr die Schulungen sowie das 2010 ausgelaufene LuSI-Projekt weitergeführt respektive kontinuierlich verfeinert und ausgebaut.

Über die Jahre wurde die Koordinierung der Schulungen ständig professionalisiert. Derzeit sind 15 Trainer für BEE SECURE aktiv. Sie haben sich dazu verpflichtet, die Botschaften und pädagogischen Inhalte von BEE SECURE auf eine interaktive Art und Weise an ihr Publikum weiterzugeben. Jedes Schuljahr werden alle Septima-Klassen des Landes abgedeckt. Anfragen anderer Altersstufen (der Sekundar- und der Grundschulen) werden ebenfalls erfüllt. **Im Jahr 2012 wurden so insgesamt 380 Sekundar- und 180 Grundschulklassen**, davon ein Drittel Cycle 3 und zwei Drittel Cycle 4 **sensibilisiert**. Daneben werden spezielle Themenabende für Eltern, Jugendhäuser, „Maisons relais“, Senioren und weitere Institutionen kostenfrei angeboten.

Ablauf der Schulung

Eine BEE SECURE Schulung dauert 90 Minuten (2 Schulstunden), aufgeteilt in zwei Blöcke von je zirka 45 Minuten, getrennt durch eine kurze Pause. Bei seiner Ankunft in der Klasse findet der BEE SECURE Trainer in der Regel einen Karton mit pädagogischem Material und Fragebögen vor, der im Vorfeld an die Schule geliefert wurde. Während der gesamten Schulung ist auch der Lehrer anwesend, in dessen Schulstunde der Kursus fällt.

Um einen schnellen Einstieg in die Klasse zu gewährleisten, beginnen die meisten Trainer mit einer sehr kurzen Vorstellung von BEE SECURE und dem Programm der Schulung. Dann werden die Schüler nach ihren eigenen Internetgewohnheiten gefragt: „Wie verbringt ihr eure Zeit im Internet?“ „Welche Seiten besucht ihr am meisten?“ „Welche Themen

¹ Cyberworld Awareness & Security Enhancement Services, www.cases.lu

interessieren euch besonders?“. Dies ermöglicht dem Trainer, schnell einen ersten Eindruck des Wissensstandes der Klasse sowie der Klassendynamik zu erhalten.

Die Schulung selbst ist modular aufgebaut und erlaubt somit eine individuelle Anpassung an die jeweilige Klasse und eine relativ freie Auslegung der Themenschwerpunkte. Angefangen wird jedoch immer mit einer kurzen (10 – 15 Minuten) Einführung in die technischen Aspekte. Hier werden die Jugendlichen über Viren, Würmer und Trojaner aufgeklärt (technische Schwachstellen), und wie man sich mit den technischen Maßnahmen (Antivirus, Firewall, Backups,...) vor ihnen schützen, beziehungsweise sich gegen sie wehren kann. Die Erfahrung hat gezeigt, dass die technischen Schutzmaßnahmen zwar wichtig sind, der stärkste Einfluss auf die Informationssicherheit jedoch vom Verhalten des Benutzers ausgeht (menschliche Schwachstellen). Deshalb widmet sich der Großteil der Schulung dem korrekten und möglichst sicheren Verhalten am Computer und im Internet.

Abgedeckt werden dabei Themen wie: Passwörter, (illegale) Downloads, Chats und soziale Netzwerke, gängige Betrugsmaschen und Cybermobbing. Bei Bedarf und auf Wunsch der Schüler kann das eine oder andere Thema vertieft werden. Gerne ergreifen die Schüler die Gelegenheit, um Themen anzusprechen, mit denen sie gerade konfrontiert sind. Dabei zeichnet sich dem Trainer ein reales Bild der aktuellen Situation von Schülern bezüglich Computer- und Internetgewohnheiten ab. Am Ende der Schulung erhalten sowohl Schüler als auch Lehrer einen Evaluierungsbogen, der es ihnen erlaubt, das Training zu bewerten und zu kommentieren.

Jugend und Internet: die aktuelle Situation

Computer

Eine aktuelle deutsche Studie belegt, dass es mittlerweile in allen Haushalten, in denen Jugendliche wohnen, zumindest einen Computer oder Laptop gibt². Sieht man eine 2012 veröffentlichte Studie zum Gebrauch der neuen Medien von Sekundarschülern in Luxemburg ein, stellt man fest, dass im Jahr 2010 bereits über 99% der luxemburgischen Jugend ab 12 Jahren Computer und Mobiltelefon benutzten³. 2011 hatten 91% aller Luxemburger Haushalte Zugang zum Internet und 92% verfügten über mindestens einen Computer⁴.

Schon Grundschüler haben oft ihren eigenen Computer, und dieser steht nicht selten im Schlafzimmer und ist somit rund um die Uhr ohne Aufsicht nutzbar. 2010 hatten von über 1.500 befragten Jugendlichen 49,4% (Schüler der „septième“) respektive 67,1% (Schüler der „onzième“ und „troisième“) ihren Computer im eigenen Zimmer stehen.⁵ Bereits an diesem,

² Jim-Studie2012, Medienpädagogischer Forschungsverband Südwest, <http://www.mpfs.de/index.php?id=537> (14.01.2012)

³ Paulos/Duscherer: „Luxembourg New Media Survey 2010“

⁴ Le Luxembourg en chiffres, 2012, 50 ans statec

⁵ Paulos/Duscherer: „Luxembourg New Media Survey 2010“

sich häufenden Phänomen zeichnet sich die Sorglosigkeit vieler Eltern bezüglich des Internetkonsums ihrer Kinder ab. **Einerseits gibt es häufig kein Bewusstsein für die Gefahren der neuen Medien, andererseits besteht die Gefahr, dass der Computer bewusst oder unbewusst als „Babysitter-Ersatz“ fungiert.**

Ihren Computer nutzen die meisten Jugendlichen täglich während durchschnittlich etwa 2 Stunden; am Wochenende und mit zunehmendem Alter noch länger. Dies in erster Hinsicht zum Arbeiten, beziehungsweise Erledigen der Hausaufgaben (inklusive Informations-Recherchen im Internet), und zur Unterhaltung. Letztere finden sie auch größtenteils im Internet, sei es in sozialen Netzwerken, Foren, Chats, auf Video- oder auf Spieleseiten. Offline wird der Computer zur Spielkonsole und zum Musikplayer.⁶

Der Trend geht dennoch ganz klar in Richtung mobile Geräte. Kein Wunder, denn Smartphone oder Tablet-PC sind immer dabei, leicht bedienbar und sofort benutzbar. Das macht sich in der Wirtschaft auch in den sinkenden Absatzzahlen von Desktops oder Laptops bemerkbar, die nur schwer mit der mobilen Konkurrenz mithalten können.

Mobiles Internet

Handys besitzen die meisten jungen Luxemburger schon in der Grundschule. Den BEE SECURE Trainern fällt während der Schulungen auf, dass so gut wie alle „septième“-Schüler (also 12-jährige Kinder) nicht bloß ein reguläres Mobiltelefon, sondern gleich ein professionelles Smartphone besitzen. **„Wenn ein Kind mal kein Smartphone hat, dann aus finanziellen Gründen, oder weil die Eltern sehr strenge Prinzipien haben – was eher selten vorkommt“**, so die Aussage eines erfahrenen Trainers. Ihr Smartphone benutzen die Kinder dann auch gerne, um uneingeschränkt im Internet zu surfen, auf Facebook aktiv zu sein, Musik zu hören, Fotos und Videos aufzunehmen, die verschiedensten Apps herunterzuladen und per SMS zu kommunizieren.

Was Eltern leider oft vergessen: Smartphones sind kleine, aber vollwertige Computer für die Hosentasche. **Haben die Eltern oft noch einen prüfenden Blick auf den Heimcomputer, so entfällt beim Smartphone meist jegliche Kontrolle.** Hier gibt es derzeit keine Filter, die den Nachwuchs vor pornografischen Inhalten schützen, oder den Zugriff auf Glücksspiel- oder gewaltverherrlichende Seiten unterbinden. Auch lauern beim Smartphone so einige Kostenfallen, in die viele Jugendlichen blind hineintappen. Als Reaktion darauf, und um diesen vorzubeugen, hat BEE SECURE im Dezember 2012 einen speziellen Smartphone-Flyer herausgebracht, der vor allem Jugendliche ansprechen soll und ihnen erklärt, wie sie Roaming-Kosten, Premium-SMS und In-App-Käufe im Griff haben können.

Ein weiteres Problem, das von Handys ausgeht, ist ihre Rolle als beliebtes Werkzeug für Cybermobbing. Das geht von heimlich gemachten und per Handy oder Internet verteilten

⁶ idem

Aufnahmen (Fotos, Videos), die eine Person bloßstellen über Droh-SMS bis hin zu „Happy Slapping“. Letzteres bezeichnet das Phänomen, dass eine unbeteiligte Person verprügelt wird, einzig und allein mit dem Ziel, die Prügelei per Handykamera aufzuzeichnen und zu verbreiten. **Für viele Jugendliche, vor allem für Jungs, sind brutale oder pornografische Videos auf dem Handy Statussymbole.** Wer die härtesten Filme hat, verdient den Respekt des anderen. Hierbei spielt der Gruppenzwang eine große Rolle, denn den meisten Jugendlichen ist durchaus bewusst, dass es sich bei solchen Fotos und Videos um unangebrachte bis verbotene Inhalte handelt, doch treibt sie der Wunsch, cool zu sein und akzeptiert zu werden dazu an, sie dennoch zu konsumieren.

Es sind aber auch Fälle bekannt, in denen Kinder von Mitschülern gezwungen wurden, sich pornografische oder extrem grausame Videos immer wieder anzusehen. Für die Kinder waren dies sehr schockierende Erfahrungen, und umso schlimmer, da einige von ihren Eltern für den Besitz und Konsum dieser Videos noch bestraft wurden.

Sicherheit

Schadprogramme

Zwar wissen die Jugendlichen, dass es Malware wie Viren oder Würmer gibt, die ihren Computer angreifen können, und die meisten haben auch selber schon mal ein solches Schadprogramm erwischt, dennoch wird ihr Verhalten von einer erschreckenden Naivität und Sorglosigkeit beherrscht. **Immer wieder müssen die BEE SECURE Trainer feststellen, dass Kinder Schadsoftware als ein unausweichliches Übel hinnehmen. Statt sich mit dem präventiven Schutz des Computers zu befassen, werden Warnungen und Fehlermeldungen so lange ignoriert, bis ein Schaden das Gerät unbenutzbar gemacht hat.** Erst danach wird sich gezwungenermaßen mit der Reparatur auseinandergesetzt.

Während der Schulungen erzählen die Jugendlichen, welche Erfahrungen sie mit Schadprogrammen gemacht haben. Vereinzelt wird berichtet, wie zum Beispiel ein Trojaner im Anhang einer E-Mail versteckt war, die als Hausaufgaben-Mail getarnt war und der anschließend Daten vom Computer gelöscht hat, oder wie ein Mac von einem Virus infiziert wurde und sich die Schülerin erst daraufhin ein Antivirenprogramm gekauft hat.

Die Neugierde der Jugendlichen ist groß, und wenn eine Datei ihr Interesse geweckt hat, wird sie - allen Umständen und Risiken zum Trotz – heruntergeladen. Besonders beliebt sind zum Beispiel kostenlose Webinhalte wie Spiele oder Apps, Musik- und Filmdownloads. Wegen der Viren, die sie sich damit einfangen können, machen sich die Allerwenigsten Sorgen. Kinder, die regelmäßig Filesharing betreiben, berichten immer wieder von Viren, die sie sich dabei einfangen. Ein Grund, mit den Downloads aufzuhören, ist das aber für die wenigsten.

Zwar ist der Begriff „Virus“ durchaus bekannt, jedoch weiß kaum ein Jugendlicher, wie er funktioniert, beziehungsweise welchen Schaden er anrichten kann. Wahrgenommen wird

er, wie schon angesprochen, als unausweichliches Übel, das den Computer vorübergehend außer Betrieb setzt. Welche Schwachstellen er ausnutzen kann, ist, genau wie der Zusammenhang zwischen Schadprogrammen und sensiblen Daten, den meisten unbekannt.

Schutzmaßnahmen

Aus der allgemeinen Sorglosigkeit gegenüber Schadsoftware resultiert ein entsprechend nachlässiger Umgang mit den verschiedenen technischen Schutzmaßnahmen. Die meisten Schüler wiegen sich in Sicherheit, wenn sie (in der Regel gleich nachdem ein Computer neu angeschafft wurde) ein Antivirenprogramm einmalig installiert haben. Dass dieses Programm regelmäßig aktualisiert werden muss, um zuverlässig arbeiten zu können, wird meist ignoriert. **Warnhinweise, die automatisch erscheinen, wenn für ein Programm ein Update zur Verfügung steht, werden von den Jugendlichen oft als störend und nicht dringend wahrgenommen.** Lieber wird das „nervige Popup“ schnell weggeklickt und dann weitergespielt oder gesurft. Hier setzen die BEE SECURE Trainer an und appellieren an die Schüler, dass die zwei Klicks und die Minute Wartezeit zum Installieren eines Updates durchaus gut investiert sind.

Die meisten vorinstallierten Antivirenprogramme sind kostenpflichtig. Viele Eltern scheuen jedoch davor zurück, die Versionen zu bezahlen. Sie schätzen den zu erwartenden Schaden für die Kinder sehr gering ein, da sie ja kaum über materielle Werte verfügen. **Doch auch wenn Kinder kein E-Banking betreiben und keine vertraulichen Daten gespeichert haben, kann Malware einen riesigen Schaden anrichten und den Ruf ihres minderjährigen Opfers in Mitleidenschaft ziehen.** Man braucht nur an Spam-Trojaner zu denken, an Passwort-Hacking und daraus resultierende Verleumdung oder das Ausnutzen des Computers durch Dritte für kriminelle Aktivitäten.

Nicht nur Jugendliche haben große Wissenslücken bezüglich der technischen Aspekte in der Informationssicherheit. Auch während der Schulung von Erwachsenen fällt den Trainern immer wieder auf, dass viele zum Beispiel den Unterschied zwischen Antivirus und Firewall nicht kennen, oder nicht wissen, wie und warum man Backups seiner Dateien durchführen sollte.

Immer wieder stellen die BEE SECURE Trainer jedoch fest, dass es in einer Klasse durchschnittlich 1 bis 2 Schüler gibt, die außerordentlich gut informiert sind. Diese geben meist an, von ihren Eltern über den Umgang mit dem Computer aufgeklärt worden zu sein. Ab und zu treffen die Trainer auch auf kleine Programmier-Experten, die schon ihre eigenen Programme schreiben und zum Beispiel wissen, wie Bluetooth oder ähnliche Anwendungen funktionieren. Leider sind sie in der absoluten Minderheit und eine große Kluft trennt sie von ihren doch eher unaufgeklärten und naiven Altersgenossen. Hier zeichnet sich ab, welchen großen Einfluss die Eltern auf das Computer- und Onlineverhalten ihrer Kinder haben können.

Internetnutzung

Das Internet dient den Jugendlichen nicht nur als Informationsquelle, sondern in hohem Maße auch zur Selbstdarstellung. Das zeigen Profile auf sozialen Netzwerken wie Facebook. Hier hat jeder die Möglichkeit, sich nach außen so zu zeigen, wie er wahrgenommen werden will. **Unter den Jugendlichen herrscht ein großer Druck, möglichst cool (hauptsächlich Jungen) oder begehrenswert (hauptsächlich Mädchen) rüberzukommen.** Ob sie ihr Ziel erreicht haben, merken sie schnell, denn auf den meisten interaktiven Internet-Plattformen (Facebook, Flickr,...) haben die User die Möglichkeit, Beiträge von anderen zu bewerten. Ein fragwürdiger Trend, denn längst ist daraus ein Wettstreit nach den meisten „Likes“, Klicks oder Komplimenten entstanden. Wer Pech hat, oder die falschen Inhalte hochlädt, muss hingegen mit scharfer Kritik und Beleidigungen rechnen – ein Phänomen, das bei mangelndem Selbstbewusstsein tiefe Kratzer im Ego eines Kindes hinterlassen kann! **Das Internet ist erbarmungslos und der Grat zwischen „Hero“ und „Loser“ oft sehr schmal. Dass Jugendliche dennoch der Faszination verfallen, daran teilhaben zu wollen, oder aus einem Gruppenzwang heraus zu müssen, verstärkt den Ruf nach einer pflichtbewussten Medienerziehung.**

Soziale Netzwerke (Facebook)

Facebook gehört bei den Jugendlichen zu den am meisten genutzten Internetanwendungen. **Schon in der Grundschule haben viele Kinder ab 10 Jahren einen Account bei Facebook** (auch wenn dies eigentlich erst ab 13 Jahren erlaubt ist). Auf „septième“ ist es dann schon mindestens die Hälfte der Klasse, manchmal auch die gesamte. Sogar wenn die Eltern es den Kindern verbieten, melden sie sich bei Facebook an, und sei es nur, um dazuzugehören. Problematisch wird dies spätestens dann, wenn die Kinder auf Probleme treffen, und sich ihren Eltern nicht anvertrauen können.

Beim Facebook-Konsum lässt sich eine gewisse Abhängigkeit von den herrschenden Sozialstrukturen feststellen. Generell merken die Trainer, dass Kinder mehr Zeit in sozialen Netzwerken verbringen, wenn beide Elternteile berufstätig sind, beziehungsweise wenig Zeit für sie haben. Facebook wird dann zum Ersatz für den fehlenden Sozialkontakt in der realen Welt. Auch für finanziell schlechter gestellte Kinder, deren Eltern sich keine Hobbies für sie leisten können, bietet Facebook mit seinen unzähligen Spielen, Chatmöglichkeiten und Fanseiten eine leicht zugängliche Alternative der Freizeitbeschäftigung. Darüber hinaus sind in der Hauptstadt mehr Jugendliche auf Facebook aktiv, als zum Beispiel in den ländlichen Gebieten.

Die Freundesliste auf Facebook ist für die meisten Jugendliche ein Statussymbol, beziehungsweise eine Beliebtheitsskala. Je mehr Freunde man auf Facebook hat, umso cooler ist man. Dementsprechend werden oft auch Fremde und den Kindern gänzlich

unbekannte Personen als Freunde akzeptiert und erhalten somit Einblicke in die Privatsphäre der Jugendlichen. Mit letzterer gehen die meisten leider sehr fahrlässig um. Das bezeugen auch die Aussagen der Schüler, die während der BEE SECURE Schulung immer ein großes Interesse am Thema Facebook haben.

Fast alle haben schon Erfahrungen mit Facebook-Einträgen gemacht, die sie selber oder eine andere Person bloßgestellt haben (Mobbing über Facebook). **Einige veröffentlichen blauäugig ihre Privatadresse, Handynummer und weitere Kontaktdaten.** Auch ist den meisten nicht bewusst, wie zum Beispiel ein veröffentlichtes Geburtsdatum, die Angabe der Schule und ein mehr oder weniger anzügliches Profilfoto dazu führen können, dass sie von Fremden belästigt und im schlimmsten Fall auch im realen Leben verfolgt werden können. Besonders junge Mädchen zeigen sich gern provokativ kokett auf ihren Facebook-Seiten. **Leichtfertig und naiv veröffentlichen schon 12-Jährige relativ freizügige Fotos von sich im Internet und freuen sich dann über „Likes“ oder Komplimente.** Von den BEE SECURE Trainern darauf angesprochen, verstehen sie oft nicht, was schlimm daran sein soll. Gepaart mit der Tatsache, dass die meisten Jugendlichen auch Fremde als „Freunde“ annehmen, und keine Ahnung von den geltenden Privatsphäre-Einstellungen haben, ist dies besonders gefährlich.

Oft schildern Mädchen von Facebook-Bekanntschaften, die sich als „ältere Herren“ mit eindeutig sexuellen Absichten herausstellen. Per Privatnachricht werden viele aufgefordert, erotische Bilder von sich zu verschicken, oder aber erhalten selber anzügliche Fotos, was noch verstörender ist. In sehr vielen Klassen erzählen die Jugendlichen, Facebook-Bekanntschaften, die sie im realen Leben nicht kennen, hätten sie zu einem privaten Treffen aufgefordert. Ein Mädchen erzählte sogar, beim Chat mit einem vermeintlich 16-jährigen Facebook-Freund (der sich später als Mitt-Vierziger herausstellte) sei plötzlich ihre Webcam angegangen. Das ist durchaus möglich, wenn der „Freund“ ihr vorher einen Trojaner auf den Computer geschickt hat. BEE SECURE appelliert deshalb immer klar und deutlich, dass man sich nie (schon gar nicht ohne elterliche Begleitung) mit Leuten treffen darf, die man nur aus der virtuellen Welt kennt und ruft die Jugendlichen dazu auf, suspekten „Freunden“ zu melden, die „Freundschaft“ sofort zu beenden und mit einer Vertrauensperson über unangenehme Situationen im Internet zu sprechen.

Facebook wird bei den Schülern allerdings nicht nur als Mittel zur Selbstdarstellung genutzt, sondern auch als eine Art „Rache-Plattform“. **Streitigkeiten, die früher im Pausenhof geregelt wurden, werden nun wortstark auf Facebook ausgefochten („Flaming“).** Die Täter handeln oft im Affekt, fügen ihren Opfern jedoch erheblichen Schaden zu, da das Geschriebene oder ein veröffentlichtes Foto im weltweiten Netz herumschwirrt und sogar nach dem Löschen auch noch Jahre später unverhofft wieder auftauchen kann. Regelmäßig erreichen in diesem Kontext die BEE SECURE Helpline Anfragen von Schülern und Eltern.

Ein häufiges Problem auf Facebook sind auch Fake-Profilen. Hierbei handelt es sich um gefälschte Profilseiten, mit dem Ziel, andere auszuspionieren und selbst unerkannt zu bleiben,

beziehungsweise im Namen eines Anderen Unfug zu posten. Ein Mädchen erzählte während der Schulung, jemand habe ihr Foto als Profilbild bei Facebook verwendet. Sie hatte sich ihrer Mutter anvertraut und dann denjenigen angeschrieben, er solle das Bild löschen, ansonsten würden sie die Polizei einschalten. Die Person hat das Bild des Mädchens daraufhin entfernt. Zwei andere Schülerinnen hatten ein Fake-Profil angelegt, um über diesen Weg die Lehrer auf Facebook unerkant als Freunde zu gewinnen. Ein oft gesehener „Streich“ ist auch, dass Schüler Fake-Profile ihrer Lehrer anlegen, um sich über sie lustig zu machen. Über die rechtlichen Konsequenzen, die ein solches Handeln haben kann, machen sie sich keine Gedanken.

Ein Schüler berichtete dem BEE SECURE Trainer, er habe „aus Spaß“ ein Foto von sich mit Hitlergruß auf Facebook veröffentlicht. Daraufhin wurde er von Nazis kontaktiert, was ihn doch sehr erschreckt hatte. Ein Mädchen hatte eine Party über Facebook organisiert und nicht gemerkt, dass sie die Veranstaltung als „öffentlich“ gekennzeichnet hatte. Erst als Unbekannte auf der Feier auftauchten, wurde ihr der Fehler bewusst. Zwei weitere Beispiele dafür, wie wenig sich Kinder mit den Konsequenzen ihres virtuellen Handelns auseinandersetzen.

Ein großes Problem besteht darin, dass die Jugendlichen entweder ein leicht zu erratendes Passwort für ihre Internetanwendungen benutzen, oder aber dieses Passwort freiwillig an Freunde weitergeben. **Zahlreich werden BEE SECURE Fälle berichtet, in denen sich Außenstehende in das Facebook-Profil eines Schülers gehackt haben, und in dessen Namen Fotos und beleidigende Kommentare oder Gerüchte veröffentlicht haben.** Berichte dieser Art häufen sich zusehends!

Auch beschweren sich die Schüler immer wieder darüber, wie undurchsichtig Facebook ist. Zwar ist es ein Kinderspiel, sich anzumelden, jedoch sind die Privatsphäre-Einstellungen nur sehr schwer verständlich und oft sind Beiträge für jeden sichtbar, obwohl dies nicht von den Kindern beabsichtigt ist. Viele wissen auch nicht, wie sie sich bei Facebook abmelden und ihr Profil endgültig löschen können.

Chat

Virtuelle Chaträume werden von Jugendlichen nach wie vor gerne besucht. MSN war noch vor wenigen Jahren eines der beliebtesten Kommunikationsmittel, wurde aber zusehends von der Chatfunktion bei Facebook und Skype sowie Chat-Apps für mobile Geräte abgelöst. Auch hier sind die Jugendlichen oft wenig wählerisch, wenn es um die Auswahl und Bestätigung ihrer Freunde geht. **Während der Schulungen erzählen die Kinder, dass sie auf den Freundeslisten von Freunden nach neuen Kontakten stöbern, um mit ihnen zu chatten – auch wenn es für sie eigentlich Fremde sind.** Derzeit der Renner sind Anwendungen wie z.B. „WhatsApp“, bei denen Benutzer über Smartphone in Echtzeit Nachrichten austauschen

können. Chatten kann man bei den meisten Apps dieser Art nur mit Leuten, deren Telefonnummer man im Gerät gespeichert hat.

Genau wie bei Facebook sehen sich auch im Chat hauptsächlich Mädchen mit sexueller Belästigung konfrontiert. Zwei Mädchen erzählten einem BEE SECURE Trainer jedoch, wie sie absichtlich einen Pädophilen im Chat „angemacht“ hatten, und seiner Anfrage für ein Treffen nachgekommen seien, nur um ihm aus dem Hinterhalt aufzulauern und sich über ihn lustig zu machen. Zwei andere Mädchen hingegen berichteten von Fremden, die sie zum Strippen vor der Webcam überreden wollten.

Immer wieder kommt es vor, dass Jugendliche erzählen, wie sie sich mit Chatbekanntschaften getroffen haben. Hier rufen die BEE SECURE Trainer zu äußerster Vorsicht auf und erinnern daran, dass im Internet nicht jeder der ist, der er zu sein behauptet. Es gibt natürlich auch Positivbeispiele: Häufig erwähnen Jugendliche, dass sie eine Chat-Bekanntschaft blockiert haben, nachdem sie angefangen hat, nach privaten Dingen zu fragen.

Oft wird deutlich, dass die Jugendlichen im Chat nicht bloß eine nette Unterhaltung suchen, sondern einen „Kick“. Ein gutes Beispiel dafür ist „Chat Roulette“, das gelegentlich während der BEE SECURE Schulung angesprochen wird. Hierbei handelt es sich um weltweite Chats per Webcam, bei denen ein Zufallsgenerator über den Chatpartner entscheidet. Längst ist das Programm als Sammelstelle für Exhibitionisten und Perverse in Verruf geraten, was allerdings wenig an seiner Beliebtheit ändert. Auch in Luxemburg treffen sich Teenager gerne, um als Gruppe im Chat Roulette ihren „Spaß“ zu haben. Allein trauen sich jedoch die wenigsten vor die Webcam. Kein Wunder, denn laut ihren Aussagen handelt es sich bei mehr als der Hälfte der Chatpartner um fragwürdige Gestalten, bei denen man damit rechnen muss, dass sie ihre Geschlechtsteile vor der Kamera entblößen.

Neben dem Videochat mit Fremden per Zufallsgenerator gibt es noch andere, neuere Trends die das Internet von den USA oder Asien her erobern. Noch sind sie in Luxemburg wenig bekannt, doch ist es in der Regel nur eine Frage der Zeit, bis sie auch in die Kinderzimmer hierzulande Einzug halten. „YouNow“ zum Beispiel ist ein Streamingportal, das hauptsächlich von Kindern und Jugendlichen ab 12 Jahren – meist ohne elterliches Wissen – benutzt wird. Mit wenigen Klicks kann jeder ein paar Minuten Ruhm genießen, vorausgesetzt er verfügt über eine Webcam und hat keine Angst, sich vor einem Livepublikum zu zeigen und schlimmstenfalls zu blamieren. Wie der User seine Zuschauer während seiner Live-Session zu unterhalten gedenkt, ist ganz ihm selbst überlassen. Das Tückische an diesem Konzept: die Zuschauer bewerten, ob ihnen die Darbietung gefällt, oder nicht. So kann man sich mit vielen „Likes“ Extra-Minuten, also mehr Live-Sendezeit verdienen, die wiederum durch Geldpreise belohnt wird.

E-Mail

Als reines Kommunikationsmittel unter Jugendlichen wurde die E-Mail längst von sozialen Netzwerken (die ebenfalls die Funktion bieten, Nachrichten zu verschicken) und SMS (viele

Jugendliche haben Flatrates und können unbegrenzt SMS verschicken) vom Thron gestoßen. **E-Mails zu verschicken gilt als bieder und nicht reaktiv. Den einzigen Vorteil, den Jugendliche in der E-Mail sehen, ist die Möglichkeit, Datenanhänge zu versenden, was dann zum Beispiel für Gruppenarbeiten in der Schule genutzt wird.** Über eine eigene E-Mail-Adresse verfügen quasi alle Jugendlichen, nicht zuletzt, da sie eine Voraussetzung zur Anmeldung bei den meisten Internetanwendungen ist.

Bei der Weitergabe ihrer E-Mail-Adresse sind die Jugendlichen relativ großzügig und hinterfragen nicht viel. Daraus resultiert, dass sie große Mengen an Spam erhalten sowie Ketten-E-Mails und dubiose Nachrichten von unbekannten Absendern.

Die BEE SECURE Trainer ermahnen die Schüler zu einem vorsichtigen Umgang mit E-Mails und klären sie über ihre Rolle als Verteiler von Schadsoftware auf. Die Grundregeln im Umgang mit E-Mails lauten unter anderem: „Datenanhänge vor dem Öffnen auf Viren prüfen“, „Nicht auf Links in E-Mails klicken“, „Keine geheimen Daten aufgrund einer E-Mail preisgeben“ und „Niemals auf Spam antworten“.

Seit einiger Zeit lässt sich beobachten, dass bei einigen Jugendlichen die E-Mail-Adresse kaum noch wahrgenommen wird. Zwar ist eine E-Mail-Adresse nötig um sich auf einer sozialen Plattform (Facebook, MSN,...) anzumelden, aber nach dem Anmelden verlagert sich die Kommunikation rein auf die sozialen Netzwerke. Die Jugendlichen sind zumeist ständig eingeloggt, und haben dann verdrängt, dass sie sich eigentlich mit einer E-Mail-Adresse angemeldet haben. Das Passwort zum Abrufen der E-Mails (und damit zur Kontrolle über ihre anderen Online-Accounts) rutscht schnell in den Hintergrund.

Passwörter

Generell fällt auf, dass die Jugendlichen sehr nachlässig mit ihren Passwörtern umgehen. Das fängt schon bei der Auswahl derselben an: Statt sich an die Basisregeln zu halten (leicht zu merken – schwer zu erraten, Groß-, Kleinbuchstaben und Sonderzeichen benutzen), entscheiden sie sich oft für einfache Zahlenkombinationen wie das eigene Geburtsdatum oder Namen. **Außerdem wird meist für eine ganze Palette von Internetanwendungen ein und dasselbe Passwort benutzt.** Die Quittung sind gehackte MSN- und E-Mail-Accounts und Facebook-Profile. Ein weiteres Phänomen: **Oft geben Jugendliche ihr Passwort im Vertrauen an Freunde weiter.** Ist die Freundschaft dann einmal vorüber, oder das Passwort auf sonstigem Weg durchgesickert, ist das Entsetzen groß. Die BEE SECURE Trainer können regelrecht ein Lied singen über Jugendliche, deren virtuelles Leben aus den Rudern gelaufen ist, nachdem sich andere Zugriff auf ihre Konten verschafft und in ihrem Namen (böswillige) Kommentare veröffentlicht haben. Sie bemühen sich, den Jugendlichen klar zu machen, wie wichtig ein gutes Passwort ist, und wie wichtig es ist, dieses geheim zu halten.

Mit der Zahnbürstenkampagne aus dem Jahr 2009 verfügen die Trainer über eine einprägsame Metapher, die auch in den Schulungen weiterhin gut ankommt: „Passwörter sind wie Zahnbürsten: Sorgfältig auswählen, regelmäßig wechseln, nicht teilen und unbedingt benutzen“.

Recht am eigenen Bild

Es ist unter den Schülern gang und gebe, sich gegenseitig zu fotografieren, und die Bilder dann ins Internet, etwa auf Facebook, hochzuladen. Dass man dafür eigentlich das Einverständnis der abgebildeten Person braucht, wissen sie nicht. **Insgesamt ist den meisten nicht bewusst, welche Rechte sie auf ihren eigenen Inhalten beziehungsweise auf ihre eigene Privatsphäre haben.** Immer wieder reagieren sie überrascht, wenn die BEE SECURE Trainer sie darüber aufklären, dass sie eigentlich selber entscheiden dürfen, welche privaten Daten von ihnen veröffentlicht werden, beziehungsweise, wie sie sich anstellen müssen, um im Streitfall ihr Recht einzufordern.

Seit 2010 benutzt BEE SECURE bei Aktionen Polaroid-Kameras, um die Bevölkerung mit einem Gegenteilbeispiel („ein Polaroid-Foto erhalten Sie an Ort und Stelle auf die Hand, es ist nirgends gespeichert und kann nicht vervielfältigt werden“) auf die Unüberschaubarkeit der digitalen Fotografie aufmerksam zu machen. 2012 wurde eine weitere Aktion zum Thema Bildrechte mit großem Erfolg eingeführt: Vor einer Fotowand ließen sich Besucher in der Erwartung eines Erinnerungsporträts ablichten. In Wahrheit wurde jedoch nur ihr Gesicht digital herausgeschnitten und auf den Körper einer nicht sehr ansehnlichen Gestalt geklebt. Dies mit der Botschaft: „Wer sich digital fotografieren lässt, hat keine Kontrolle darüber, was mit dem Bild passiert“.

Die BEE SECURE Trainer haben es sich zur Aufgabe gemacht, **den Jugendlichen den Balanceakt zu vermitteln zwischen Fotos machen und verteilen um „cool“ und in der Gruppe angesehen zu sein und dem übermäßigen und unbedachten Bloßstellen in sehr persönlichen oder peinlichen Momenten.**

Urheberrecht

Bezüglich Urheberrechte machen sich die Jugendlichen kaum Gedanken. Zwar wissen sie von ihren Lehrern, dass man nicht einfach Bilder oder Texte für Hausaufgaben aus dem Internet kopieren darf, ohne diese als Zitate zu kennzeichnen und mit Quellennachweisen zu vermerken, jedoch ist ihr Wissen in der Regel auch schon hierauf beschränkt.

Ein Mangel an Verständnis von Urheberrecht wird auch deutlich, wenn man sich ansieht, mit welcher Leidenschaft und Überzeugung sich Jugendliche Filme und Musik von oft dubiosen Seiten im Internet herunterladen. Es besteht zwar ein gewisses Interesse an den legalen Alternativen, denn die BEE SECURE Trainer stellen fest, dass aktiv von den Schülern danach

gefragt wird. Jedoch lädt nur ein relativ kleiner Teil von Schülern solche Inhalte legal auf vertrauenswürdigen Webseiten herunter und bezahlt auch dafür. Es handelt sich hierbei meist um Kinder, deren Eltern die Thematik mit ihnen besprochen haben, und das Geld für die legalen Downloads zur Verfügung stellen.

Für die anderen bedeutet „Filesharing“ lediglich ein gewisses Risiko, sich einen Virus einzufangen, oder aber statt des erhofften Blockbusters einen getarnten Porno herunterzuladen. Dass sie die Künstler um einen Teil ihres Verdienstes betrügen, sehen sie nicht ein, und auch vor einer eventuellen gerichtlichen Verfolgung haben sie keine Angst. Im Gegenteil, **sich illegal Inhalte herunterzuladen, gilt als Kavaliersdelikt. „Illegal“ steht stellvertretend für „cool“.**

Cybermobbing

Die aktuelle Kampagne von BEE SECURE, „NOT FUNNY – BEE FAIR“ befasst sich ganz mit dem Kampf gegen Cybermobbing. Das Thema ist nicht zufällig gewählt, denn regelmäßig erreichen BEE SECURE Anfragen und Hilfesuche von betroffenen Schülern, Lehrern oder Zeugen, und dies bereits im Grundschulalter.

Am Thema Cybermobbing haben die Jugendlichen ein großes Interesse. Nicht zuletzt, da allen dieses Phänomen bekannt ist. Wenn nicht direkt als Opfer oder Täter, dann doch zumindest als Zeuge. Immer wieder berichten sie auch von Fällen, die sie aus den Medien kennen – Fälle, in denen das Opfer die einzige Flucht im Selbstmord sah. Gerade solch traurigen Ereignisse berühren die Schüler und hinterlassen einen bleibenden Eindruck. Gegenüber den Trainern zeigen sie sich schockiert über Mobbing und solidarisch mit dem Opfer. **Viele erzählen von ihren eigenen Erfahrungen: Hass-Gruppen gegen eine bestimmte Person auf Facebook, Drohungen und Erpressungen per SMS, veröffentlichte Beleidigungen, peinliche Videos und Fotos, auf Netzwerken verbreitete Gerüchte,...**

Ein Lehrer berichtete von einem Fall, bei dem ein Schüler heimlich beim Urinieren gefilmt, und dieses Video digital verbreitet wurde. In einer anderen Schule haben zwei Kinder die Klasse gewechselt, nachdem sie das Mobbing nicht mehr ausgehalten haben. **Viele Kinder sind der Meinung, sich ihren Eltern in solch einem Fall nicht anvertrauen zu können.** Erschwerend zum klassischen Mobbing auf dem Schulhof kommt nämlich noch hinzu, dass die Eltern meist gar nicht nachvollziehen können, wie das virtuelle Leben ihres Kindes aussieht; das heißt, auf welchen Webseiten es aktiv ist, wer dort seine Freunde sind, und wie der Umgangston untereinander ist. Vielen Eltern ist auch gar nicht bewusst, wie wichtig ihrem Kind diese virtuelle Welt ist, und dass dort auf der Suche nach Anerkennung genau wie in der realen Welt auch mal mit harten Waffen gekämpft wird.

Beim Cybermobbing geraten Situationen schnell außer Kontrolle. Die Devise lautet „Einmal im Netz – immer im Netz“. Ob ein Inhalt nun versehentlich oder mit voller Absicht im Internet

gelandet ist, spielt dann keine Rolle mehr. Besonders Bilder und Videos kommen schnell in Umlauf und die ganze Welt kann daran teilhaben.

Das Schlimmste am Cybermobbing: Dank Handys, Smartphones und Internet ist man der Angst 24 Stunden am Tag während 7 Tagen in der Woche ausgeliefert. Opfer erstarren vor Panik, jedes Mal wenn ihr Handy klingelt, eine Benachrichtigung bei Facebook aufleuchtet oder der Posteingang neue E-Mails ankündigt. Kann man Mobbing in der „realen“ Welt wenigstens dann entfliehen, wenn man sich vom Täter entfernt (zum Beispiel von der Schule nach Hause kommt), ist man bei Cybermobbing an keinem Ort und zu keiner Tageszeit wirklich sicher. Opfer leiden so zum Beispiel unter schlaflosen Nächten, da sie nicht auf die Idee kommen, wenigstens nachts das Handy auszuschalten. Cybermobbing braucht nicht einmal die physische Anwesenheit seines Opfers!

Die Rolle der BEE SECURE Trainer ist es, den potentiellen Opfern die wichtigsten Grundregeln im Umgang mit verletzenden Nachrichten oder Bildern zu vermitteln sowie auf die bestehenden Anlaufstellen zu verweisen (Eltern, Lehrer/Erzieher, BEE SECURE Helpline,...).

Die Rolle der Eltern

Für viele Eltern ist die sich rasend schnell entwickelnde Technik wie ein Buch mit sieben Siegeln. Wenn das nötige Know-how fehlt, und auch der Wille, die Zeit oder die Möglichkeit, es sich anzueignen, bleibt die virtuelle Welt ein Eiland, auf dem man sich nur schwer zurechtfinden kann. Die Kinder hingegen sind in diese Welt hineingeboren worden. Als „digital natives“, schlagen sie sich selbstbewusst ihren Weg durch den Dschungel des weltweiten Netzes. Auf Eltern wirkt dieser selbstsichere Umgang mit den neuen Medien meist sehr souverän. Die Auffassung „Mein Kind kennt sich eh besser mit Internet und Co aus, also lass ich es mal machen“ liegt also fast schon auf der Hand. **Dass in der Selbstverständlichkeit, mit der Kinder das Internet benutzen, auch eine nicht zu unterschätzende Portion Naivität, eine gefährliche Sorglosigkeit und enorme Risikobereitschaft liegen, wird leider oft ignoriert.**

Eltern sind häufig schon allein deshalb auf der Verliererseite, weil sie keine Zeit haben, beziehungsweise sich keine Zeit nehmen möchten, sich mit den Internetgewohnheiten ihrer Kinder auseinanderzusetzen. Das merken die BEE SECURE Trainer zum Beispiel, wenn sie Elternabende organisieren und nur wenige Anmeldungen erfolgen.

Eine weitere Hemmschwelle für den Ausbau des Vertrauensverhältnisses zwischen Eltern und Kind ist das Problem der doppelten Viktimisierung: Unfreiwillig konsumierte schockierende Inhalte machen ein Kind bereits zum Opfer. Teilt es seine schlechten Erfahrungen mit den Eltern, droht ihm erfahrungsgemäß oft eine Standpauke oder Bestrafung (Internet-Entzug), denn viele Eltern reagieren mit Entsetzen und wenig verständnisvoll. Dies ist einer der

Gründe, warum Kinder ungern mit Eltern oder Erziehungsberechtigten über diese Art von Problemen reden.

Eltern sollten für ihre Kinder die wichtigsten Vertrauenspersonen sein. Weil das Internet heutzutage eine große Rolle im Leben der Jugendlichen spielt, ist es unerlässlich, dass auch die Eltern sich damit auseinandersetzen. **Nur wenn sie verstehen, was ihr Kind im Internet erlebt, können Eltern potenzielle Gefahren erkennen und ihnen im Notfall adäquate Ansprechpartner sein.** Aus diesem Grund strebt BEE SECURE an, Eltern noch stärker in die Sensibilisierungskampagnen und bestenfalls auch in die Schulungen mit einzubeziehen. Jedes Jahr werden Elternabende in den verschiedensten Regionen des Landes angeboten. Eltern-Kind-Schulungen, die bislang nur in Ausnahmefällen organisiert wurden, waren jedes Mal ein großer Erfolg. Es wäre wünschenswert, an diesem Konzept festhalten und es noch weiter ausbauen zu können.

2010 erschien erstmals durch das Familienministerium und CASES in Partnerschaft mit dem „Salon du Livre de l'Enfance et de la Jeunesse“ eine Informationsbroschüre für Eltern: „Kuck mat wat deng Kanner maachen!“. Sie unterstützte Eltern in der Begleitung von Kindern und Jugendlichen durch die digitale Welt und war, gekoppelt an eine Reihe von Informationsveranstaltungen, ein riesiger Erfolg. 2013 wird diese Broschüre unter der Schirmherrschaft von BEE SECURE in einer Neuauflage erscheinen.

Die Rolle der Lehrer

Die Lehrer sollten eigentlich eine gewissenhafte Medienerziehung der Kinder anstreben. Leider ist Medienerziehung nicht als Fach im Schulplan verankert. Wenn überhaupt, wird der richtige Umgang mit Handy, Internet und anderen Medien nur am Rande in vereinzelten Klassen behandelt.

Lehrer der älteren Generation haben meist sehr wenig bis keinen Bezug zum Internet. Sie haben keine Ahnung davon, wie sich ihre Schüler die Zeit am Computer vertreiben und wenig Verständnis für ihre Web-Leidenschaft. Oft merken die BEE SECURE Trainer, dass diese Lehrer die Wichtigkeit der Schulung nicht nachvollziehen und aufgrund eines mangelnden Verständnisses die Notwendigkeit einer korrekten Medienerziehung anzweifeln.

Die jungen Lehrer sind in der Regel viel aktiver im Internet, lassen sich aber dennoch grob in zwei Gruppen aufteilen: Die einen sind ausführlich informiert, kennen sich mit Datenschutz und Informationssicherheit aus und können ihren Schülern dementsprechend ein gutes Vorbild sein, während sich das Online-Verhalten der anderen Gruppe kaum von dem ihrer Schüler unterscheidet.

Gerade wegen ihres bedeutenden Einflusses auf die Entwicklung ihrer Schüler wäre es wünschenswert, dass Medienkompetenz als Schulfach im Lehrplan verankert wird. So könnte Computer- und Informationssicherheit ein fester Bestandteil der schulischen Ausbildung

werden. Im Idealfall wäre Medienerziehung auch Teil der Lehrerausbildung. Da kein anderes Medium so dynamisch ist, und der ständigen Weiterentwicklung obliegt, wie das Internet, wäre es wichtig, die Kompetenzen durchgehend auf dem neusten Stand zu halten. Dies etwa durch regelmäßige (zum Beispiel im Zweijahresrhythmus angebotene) pflichtmäßige Schulungen, an denen die Lehrer teilnehmen müssen, damit sie ihren Schülern die entsprechenden Werte weiter vermitteln können.

Ausblick

In gerade mal zwei Jahren, in denen die Schulungen unter dem Label „BEE SECURE Training“ stattfinden, haben sie bereits einen enormen Bekanntheitsgrad erlangt. Heute treffen die Trainer in der Sekundarschule auf Kinder, deren Klasse sie bereits in der Grundschule besucht hatten, und die sich teilweise noch gut an das damals Gelernte erinnern. **Es wäre jedoch utopisch anzunehmen, dass eine einzige Schulung von 90 Minuten ausreicht, um das Internetverhalten der Jugendlichen dauerhaft sicherer zu gestalten.** Gute Tipps werden zwar zur Kenntnis genommen, doch die Erfahrung hat gezeigt, dass die Wiederholung des Gelernten und das konsequente Umsetzen in praktischen Übungen unerlässlich für einen langfristigen Erfolg sind.

Aus diesem Grund wünscht sich BEE SECURE die Einbindung der Medienerziehung in den offiziellen Lehrplan der luxemburgischen Schulen sowie eine regelmäßige Weiterbildung der Lehrer auf diesem Gebiet.

Außerdem wäre es sinnvoll, die Schulungsdauer zu verdoppeln. Das heißt, in einer ersten Schulung à 90 Minuten den Kindern wertvolle Ratschläge und Aha-Erlebnisse mit auf den Weg zu geben, und dann, etwa eine Woche später, in einer zweiten 90-minütigen Sitzung zu überprüfen, woran sich die Schüler noch erinnern können, beziehungsweise einige praktische Tests am Computer zu machen. Mit zwei Sitzungen pro Schulung wäre außerdem genügend Zeit, um alle Kinder ausreichend zu Wort kommen zu lassen, interaktiver zu sein und mehr auf spezifische Bedürfnisse einzugehen. Aktuell ist es nämlich so, dass die Klassen sich sehr aktiv am Unterricht beteiligen. Zu aktiv leider, um den engen Zeitplan einzuhalten, sodass die Trainer manchmal gezwungen sind, den Elan der Kinder zu bremsen, und sie quasi „abwürgen“. Dass dies dem Erfolgserlebnis einen Seitenhieb versetzt, versteht sich von selbst.

Im Ausland wird oft sehr erfolgreich mit Multiplikatoren gearbeitet. Auch in Luxemburg ist es vorstellbar, dass sich Lehrer verstärkt dem Thema widmen, sich aus- und weiterbilden lassen. Die BEE SECURE Schulungen sind dann eine nützliche Abwechslung zum Schulalltag, während es die Lehrkräfte selbst sind, die verstärkt medienpädagogisch tätig werden, indem sie Medien in den Unterricht mit einbinden und eigenständig die BEE SECURE Schulungen vorbereiten und nachbereiten, respektive ein ganzheitliches Konzept für ihr Schuljahr planen.

Neben dem Thematisieren der negativen Aspekte bleibt es eine wichtige Aufgabe von BEE SECURE, auch die **Vorteile der neuen Technologien herauszuarbeiten und zu fördern**. Auch in Luxemburg gibt es zahlreiche Beispiele erfolgreicher Medienprojekte. Besonders hervor sticht die „LAML-App“, eine mobile Applikation, die von Schülern aus dem Lycée Aline Mayrisch entwickelt und beworben wurde. Schüler der Ecole de Commerce et de Gestion bereiten derzeit eine Konferenz zur Handynutzung vor. Durch die Förderung solcher Projekte können die BEE SECURE Botschaften positiv vermittelt werden. Zudem wächst so eine Generation heran, die selbstbewusst mit den neuen Medien umgehen kann. Dies ist ein **wichtiger Baustein für den angestrebten langfristigen Erfolg Luxemburgs als innovativer Medienstandort**.

Kinder finden immer früher den Weg ins Internet. Längst gibt es Spieleseiten, Lernportale und Suchmaschinen für die Allerkleinsten. Deshalb wird BEE SECURE ab 2013 verstärkt Gewicht auf die Sensibilisierung von Grundschulern legen. Mit „bee.lu“ wird eine Plattform für Kinder ab 4 Jahren ins Leben gerufen. Denn **genau so wie Kinder lernen, die Straße bei Grün zu überqueren und sich zu vergewissern, dass auch wirklich kein Auto kommt, müssen sie von Anfang an die Grundregeln der sicheren Computernutzung verinnerlichen**. Das Internet entwickelt sich rasend schnell – mit ihm auch seine Gefahren! Prävention und Reaktion sind die Schlüsselwörter der Informationssicherheit. Nur durch flächendeckende Sensibilisierung aller Altersstufen können sie in die Tat umgesetzt werden.

BEE SECURE, 28.01.2013

www.bee-secure.lu

