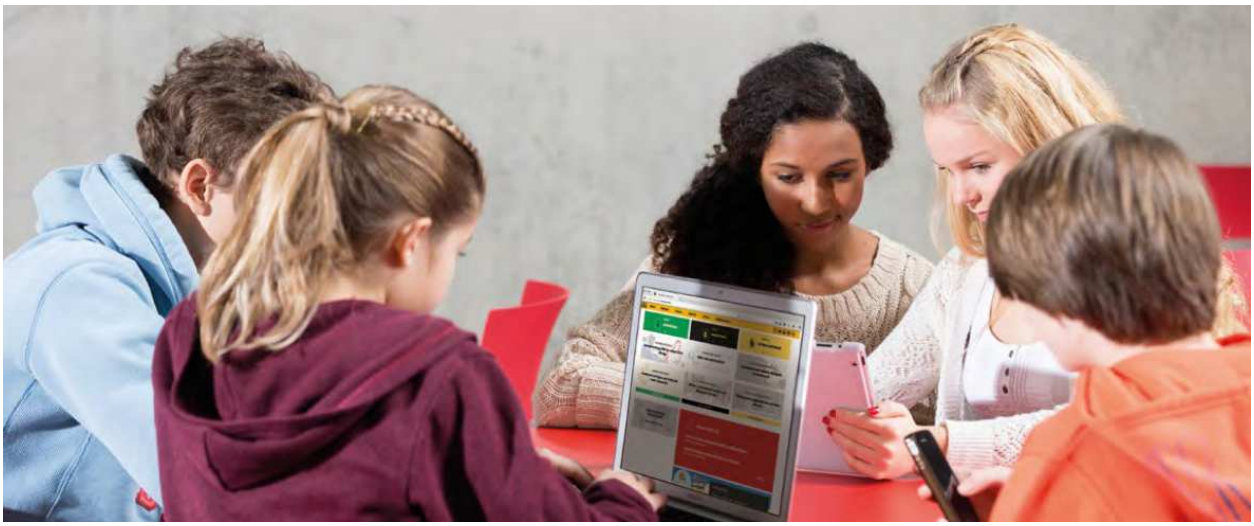
# BEE SECURE Schulungen

## Jugendliche im Umgang mit Computer und Internet

### Erfahrungsbericht für das Schuljahr 2014/2015 und 2015/2016



**Tendenzen, Probleme & Lösungsansätze**

# Inhaltsverzeichnis

# Zusammenfassung

Dieser Bericht zeichnet ein aktuelles Bild der Computer- und Internetnutzung von Kindern und Jugendlichen in Luxemburg. Es basiert auf den Erfahrungen der BEE SECURE Trainer, die im Schuljahr 2014/2015 239 Grundschulklassen, 400 Sekundarschulklassen und 100 Personen weiterer Zielgruppen, sowie im Schuljahr 2015/2016 346 Grundschulklassen, 405 Sekundarschulklassen und 59 Personen weiterer Zielgruppen sensibilisiert haben.

Kinder und Jugendliche haben fast ausnahmslos Zugang zum Internet. Neben dem Internetzugang zuhause, steht ihnen in der Schule kostenloses Internet zur Verfügung. Zudem besitzt ein Großteil der Schüler ein eigenes Smartphone, mit welchem sie auch auf mobiles Internet zurückgreifen können.

Die Handhabung von Computer, Smartphone und Co. erfordert eine **(verantwortungs-)bewusste Nutzung**. Leider kommt es aber oft zu einer **riskanten Selbstüberschätzung** bei den jungen Menschen. Viele Schüler geben zu Beginn von BEE SECURE Schulungen an, sich gut mit dem Internet auszukennen und informiert zu sein. In der Folge ergibt sich dann jedoch, dass sich die Kenntnisse oftmals wohl doch eher auf die Trends in der Onlinemedienwelt, als auf wichtige Informationen über beispielsweise Viren, Cloud oder auch die rechtliche Lage bei Fotos beziehen. Häufig sind zwar ein oder zwei Schüler pro Klasse tatsächlich gut informiert und halten sich auch gezielt autonom auf dem Laufenden, jedoch stellen diese eine Ausnahme dar. Denn bei den meisten Schülern fällt eine nicht zu unterschätzende Naivität auf. Hier setzte die Kampagne **„Clever klicken“** des Schuljahres 2014/2015 an, die über die gängigen Formen von Online-Betrug informierte und wie man sich vor den typischen Betrugsmaschen schützen kann. Die Schüler wurden dazu angeregt, das Internet mit gesundem Menschenverstand zu benutzen, denn nur wer „clever“ ist, ist verantwortungsbewusst im Internet unterwegs.

Das Schuljahr 2015/2016 stand unter der Kampagne **„Clever Cloud User“**. Sie hatte das Ziel das „Cloud Computing“ in seinen verschiedenen Facetten zu beleuchten: die positiven Seiten samt ökonomischer, technologischer und legaler Aspekte, sowie die Risiken in Bezug auf private und vertrauliche Daten. Während des Schuljahrs wurde vermehrt festgestellt, dass nur wenige Schüler etwas mit dem Wort „Cloud“ anfangen konnten.

Die KIM-Studie 2014[1], die sich mit dem Medienumgang der 6- bis 13-Jährigen in Deutschland beschäftigt, berichtet, dass Dreiviertel der 6- bis 7-Jährigen bereits erste Erfahrungen im Internet gesammelt haben. BEE SECURE Trainer bestätigen, dass diese Zahl auch für Luxemburg denkbar ist, wobei sie wahrscheinlich in den beiden letzten Jahren noch gestiegen ist. Im Durchschnitt sind 40% der 6- bis 13-Jährigen (fast) täglich online (Stand 2014), was ein Anstieg im Vergleich zu den vorherigen Jahren ist (2010: 26%; 2012: 36%). Jedoch gibt es einen großen Unterschied der täglichen Nutzung mit zunehmenden Alter: 6-7 Jahre: 15%, 8-9 Jahre: 18%, 10-11 Jahre: 38% und 12-13 Jahre: 60%. Auch hier ist mit einem Anstieg seit 2014 zu rechnen, wie die aktuelle JIM-Studie[2] zeigt.

[1] KIM-Studie 2014, https://www.mpfs.de/fileadmin/files/Studien/KIM/2014/KIM_Studie_2014.pdf
[2] JIM-Studie 2016, https://www.mpfs.de/fileadmin/files/Studien/JIM/2016/JIM_Studie_2016.pdf

Im Juli 2016 wurden für diese Studie 1.200 Jugendliche zwischen 12 und 19 Jahren aus ganz Deutschland zu ihrem Medienumgang befragt. So gaben 76% der 12- bis 13-Jährigen an, dass sie täglich im Netz unterwegs seien. Bei den 14- bis 15-Jährigen sind es 87% und bei den Älteren ist die 90%-Marke überschritten (16-17 Jahre: 93%, 18-19 Jahre: 90%). Insgesamt sind 87% der Jugendlichen zwischen 12 und 19 Jahren mindestens einmal täglich online, was ein Zuwachs von 7% seit 2015 ist.

Diese Zahlen verdeutlichen wie viel Zeit Kinder und Jugendliche im Internet verbringen und unterstreichen wie wichtig die Aufklärung für eine verantwortungsbewusste Nutzung der neuen Medien ist.

Das Internet scheint für die Jugendlichen aus zwei Gründen „überlebenswichtig" zu sein. Einerseits dient es ihnen durch die sozialen Netzwerke zur **Selbstdarstellung/(Selbst-)Bestätigung**. Jugendliche können mit verschiedenen Identitätskonzepten (cool, sexy, romantisch, stark, …) herumexperimentieren und bekommen eine direkte Rückmeldung in Form von Komplimenten oder „Gefällt mir"-Angaben wie bspw. bei Facebook. So werden sie in ihrer Selbstfindungsphase bestärkt und ein Referenzrahmen entsteht. Auf der anderen Seite dient das Internet als Kommunikationsmittel um rund um die Uhr mit Freunden in Kontakt zu bleiben oder zum Kennenlernen von neuen Menschen und zum Flirten „auf Distanz".

Diese unterschiedlichen Motivationen stehen natürlich im Zusammenhang mit dem Alter und der Entwicklungsphase der jungen Nutzer. Das damit einhergehende Verhalten ist in einem ersten Schritt sicherlich nicht direkt als riskant anzusehen, jedoch können ungeahnte Gefahren auftreten und Konsequenzen mit sich tragen. **Grooming, Sexting, Cybermobbing oder Phising** sind bspw. Risiken der Internetnutzung, die den Jugendlichen schnell zum Verhängnis werden können. Denn häufig geben sie bereitwillig persönliche Informationen preis, veröffentlichen Kontaktdaten in sozialen Netzwerken, laden uneingeschränkt Bilder hoch, die anschließend manipuliert, vervielfältigt und im weltweiten Netz verbreitet werden können.

BEE SECURE unterstreicht den **positiven Nutzen der modernen Informations- und Kommunikationstechnologien**. Kinder sollten diesen Technologien nicht alleine überlassen werden, sondern von Anfang an, die Grundregeln der sicheren und verantwortungsbewussten Nutzung verinnerlichen. Daher sind die großen Erfolge im Bereich der formalen Bildung und auf der Ebene der nationalen Kampagne sehr erfreulich. Auch die **BEE SECURE Helpline** verzeichnet einen Zuwachs in den letzten Jahren. Des Weiteren legt BEE SECURE einen Fokus auf die Elternsensibilisierung, ein Bereich der auch in Zukunft noch ausgebaut werden soll. Eltern werden in Bezug auf die Internetnutzung ihrer Kinder von BEE SECURE unterstützt, damit sie ihrer Aufsichtspflicht auch in diesem Bereich besser nachgehen können. Diesbezüglich erschien Mitte 2016 bereits die vierte, komplett überarbeitete Auflage des Elternratgebers „Kuck mat wat deng Kanner maachen!". Außerdem setzt sich BEE SECURE für eine gezielte Aus- und Weiterbildung der **Fachkräfte (Lehrer/Erzieher)** ein.

Nur wer versteht, was die Kinder und Jugendlichen online treiben, kann potenzielle Gefahren rechtzeitig erkennen und im Notfall ein adäquater Ansprechpartner sein. Daher sollte Medienerziehung zum wesentlichen Bestandteil jeder schulischen und beruflichen Ausbildung werden.

Das Internet entwickelt sich rasend schnell und mit ihm auch die Gefahren. Aus diesem Grund sind **Prävention und Reaktion** die Schlüsselwörter der Informationssicherheit. Nur durch flächendeckende Sensibilisierung aller Altersstufen kann dieses in die Tat umgesetzt werden.

## Rückblick und Ablauf der Schulungen

Seit 2008 sind die Schulungen für alle Septième-Klassen verpflichtend. Bis 2010 lief dieses unter dem Namen „Luxemburg sicher im Netz“ im gemeinsamen Programm des Ministeriums für Wirtschafts- und Außenhandel (vertreten durch CASES) und des Bildungsministeriums in Zusammenarbeit mit dem damaligen europäischen Projekt „LUSI – Luxembourg Safer Internet“.

2010 wurden die Schulungen, sowie auch die ehemaligen LuSI-Aktivitäten, an das frisch gestartete BEE SECURE übertragen. BEE SECURE ist eine gemeinsame Initiative des Ministeriums für Wirtschaft, des Ministeriums für Familie, Integration und der Großregion, sowie des Ministeriums für Bildung, Kinder und Jugend, und richtet sich an die Bevölkerung im Allgemeinen, aber im Besonderen an Kinder, Jugendliche und Familien.

Die Koordinierung obliegt dem Service National de la Jeunesse (SNJ). Die Anfragen werden per Webformular und per Telefon entgegengenommen. 8 Trainer, die das BEE SECURE Trainer Label erlangt haben, sind aktiv in den Schulen, Jugendhäusern usw. unterwegs.

Pro Schuljahr werden alle Septième-Klassen des Landes abgedeckt (verpflichtend) und stetig steigt die Anfrage für andere Altersstufen (der Grund- und Sekundarschulen). Seit dem Schuljahr 2014/2015 streben die „Technolink“-Schulen der Stadt Luxemburg und die „NorTIC“-Schulen im Norden Luxemburgs, aufgrund von Empfehlungen der IT-Zuständigen, an, die Schulung in allen Klassen des Cycle 3 und 4 durchzuführen. Bei den „Technolink“-Schulen wurden leider noch nicht alle Schüler des Cycle 3 erreicht; in den „NorTIC“-Schulen wurden die Klassen 3.1 und 4.2 geschult.

Neben der allgemeinen Schulung werden auch Schulungen zu speziellen Themen wie bspw. Cybermobbing oder eine praktische Facebook-Schulung angeboten. Des Weiteren können Themenabende für Eltern, Jugendhäuser, „Maison Relais“, Weiterbildungen für Lehrer und Erzieher, Senioren und weitere Institutionen angefragt werden, die selbstverständlich auch kostenfrei sind.

In der Regel dauert eine BEE SECURE Schulung 90 Minuten (2 reguläre Schulstunden). Während der gesamten Schulung muss auch ein Lehrer anwesend sein. Im Vorfeld wird ein Paket pro Klasse an die Schule geschickt in dem sich pädagogisches Material, Evaluierungsbögen und die Gadgets befinden.

Zu Beginn der Schulung wird zusammen mit den Schülern definiert was BEE SECURE ist und was in der Schulung behandelt wird. Dann verschafft sich der Trainer anhand von Fragen wie „Wie verbringt ihr eure Zeit im Internet?“, „Welche Seiten besucht ihr am Häufigsten?“, „Welche Themen interessieren euch besonders?“ einen Überblick über den Wissensstand der Klasse sowie der Klassendynamik.

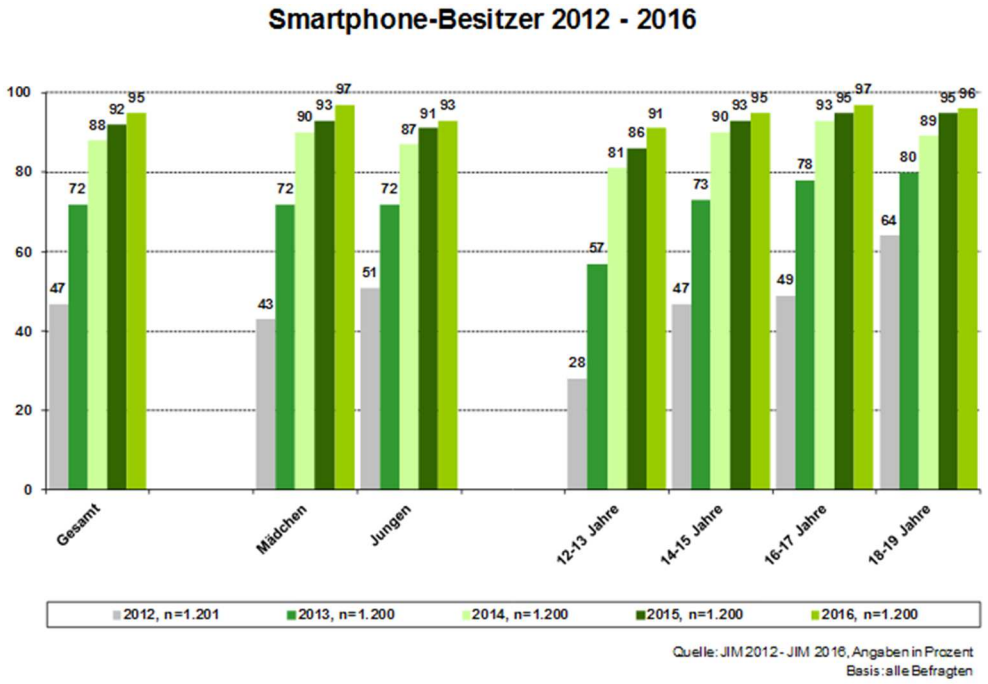
Anschließend gibt es eine kurze Einführung in die technische Infrastruktur des Internets (15-20 Minuten). Dabei werden auch die technischen Schwachstellen (Viren, Würmer und Trojaner) erklärt und wie man sich mit den technischen Maßnahmen (Antivirus, Firewall, Backups, …) vor ihnen schützt, bzw. wie man sich gegen sie wehren kann. Darauffolgt der zweite (für die meistens Schüler der wichtigere) Teil der Schulung, der sich der Vermittlung von korrektem und möglichst sicherem Verhalten am Computer und im Internet widmet. Da die Schulung modular aufgebaut ist, kann der Trainer diesen Teil sehr leicht individuell an die Schüler und an deren Themenschwerpunkte anpassen. Zu den Themen gehört unter anderem: Passwörter, Chats und soziale Netzwerke (Facebook, Instagram, Snapchat, …), Sexting, Cybermobbing, gängige Betrugsmaschen, (illegale) Downloads und Spiele. Da es ein Anliegen von BEE SECURE ist, die Schulung interaktiv zu gestalten und dieses durch das Feedback der Lehrer auch von deren Seite erwünscht ist, werden seit dem Schuljahr 2015/2016 die Themen mittels zwei Aktivitäten in Gruppenarbeit erarbeitet. Eine Aktivität beinhaltet das Entwickeln eines eigenen sozialen Netzwerkes. Die Schüler sollen sich in der Gruppe auf einen Namen und den Nutzen des sozialen Netzwerkes (z.B.: Spiele, Freunde treffen, …) einigen und eigene Regeln für dieses aufstellen. Hierbei wird zusätzlich die Kreativität der Schüler gefördert. Bei der zweiten Aktivität geht es darum, dass die Schüler sich in der Gruppe Gedanken um die Gefahren im Internet machen sollen. Sie sollen sich überlegen welche sie bereits kennen und wie man sich vor diesen schützen kann bzw. was man in so einem Fall machen kann. Weitere Gefahren werden anschließend mit dem Trainer ausgearbeitet. Während der ganzen Schulung verweist der Trainer situationsgebunden auf das aktuelle Kampagnen-Thema, welches im Schuljahr 2014/2015 „Clever klicken“ und im Schuljahr 2015/2016 „Clever Cloud“ war. Drei Hauptbotschaften werden den Schülern mit auf den Weg gegeben: „Das Internet ist keine Zauberei, sondern technische Infrastruktur.“, „Das Internet vergisst nichts.“ und „Du bist dein eigener Schutz.“. Diese Beschränkung auf drei Botschaften soll den Schülern helfen, sich die Inhalte besser zu merken. Am Ende der Schulung erhalten sowohl die Schüler als auch die Lehrer einen Evaluierungsbogen, der es ihnen erlaubt, das Training zu bewerten und zu kommentieren. Als Erinnerung wird noch ein Plakat in der Klasse aufgehängt und die Schüler bekommen Infomaterial sowie auch ein Gadget.

# Jugend und Internet

## Computer, Smartphone und Co.

Laut Statec Umfrage über die Nutzung der Informations- und Kommunikationstechnologien[3] hatten 97% aller luxemburgischen Haushalte im Jahre 2015 einen Internetanschluss. Im Vergleich zu 2010 ist dieses ein Anstieg um 7 PRozentpunkte und seit 2008 ein Zuwachs um 17 Prozentpunkte.

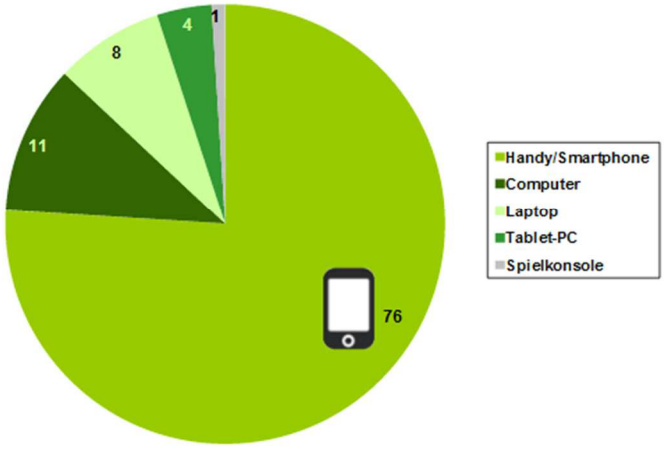
Dass die Smartphone-Besitzrate konstant steigt, zeigt die aktuelle JIM-Studie (Jugend, Information, (Multi)Media). 91% der 12- bis 13-Jährigen benutzen bereits ein Smartphone während es 2012 gerade einmal 28% waren. Zudem besitzt fast jeder Jugendlicher über 15 Jahren ein Smartphone, hingegen es im Jahre 2012 nur knapp die Hälfte war. Basierend auf den Erfahrungen der BEE SECURE Trainer ist dieses vergleichbar mit Luxemburg. Bereits Grundschüler im Alter von 6-7 Jahren sind im Besitz eines Smartphones in Luxemburg. „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 BEE SECURE Trainers. Somit sind also der individuelle und der mobile Zugang ins Internet bereits in der frühen Jugendphase vorhanden.




Eine weitere Statistik dieser Studie zeigt, dass die meisten Jugendlichen, nämlich über Dreiviertel (76%), das Smartphone benutzen um ins Internet zu gehen. Es folgt (weit abgeschlagen) der stationäre Computer (11%) und der Laptop (8%). Diese Zahlen können in etwa auch so für Luxemburg übernommen werden.

[3] Statec – Luxemburg in Zahlen 2016, http://www.luxembourg.public.lu/de/publications/c/statec-lux-chiffres2016/index.html

**Am häufigsten eingesetztes Gerät zur Internetnutzung 2016**

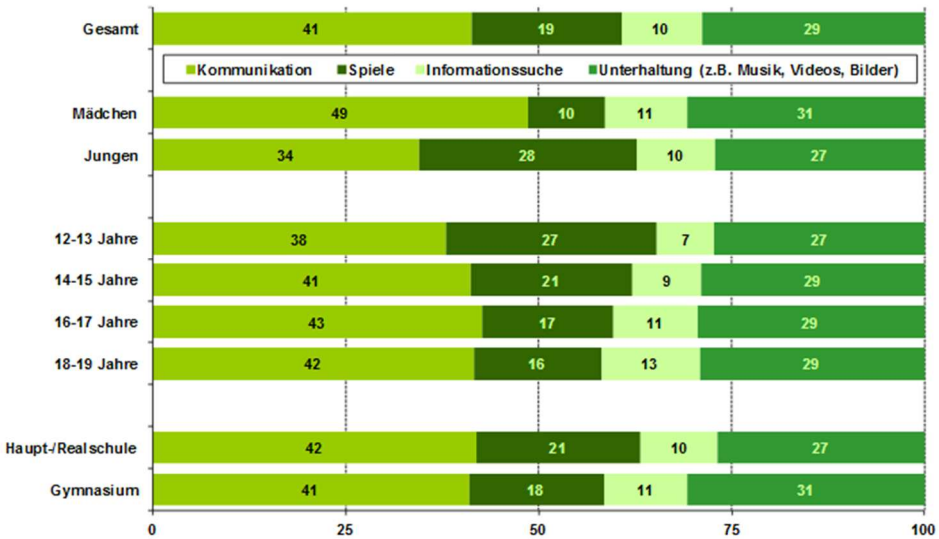



Quelle: JIM 2016, Angaben in Prozent
Basis: Befragte, die mind. alle 14 Tage das Internet nutzen, n=1.182

Betrachtet man die Nutzungsdauer des Internets innerhalb der Woche, so schätzen die Jugendlichen zwischen 12 und 19 Jahren ihre tägliche Zeitaufwendung auf etwa 200 Minuten (laut JIM-Studie 2016); am Wochenende und mit zunehmenden Alter noch länger.

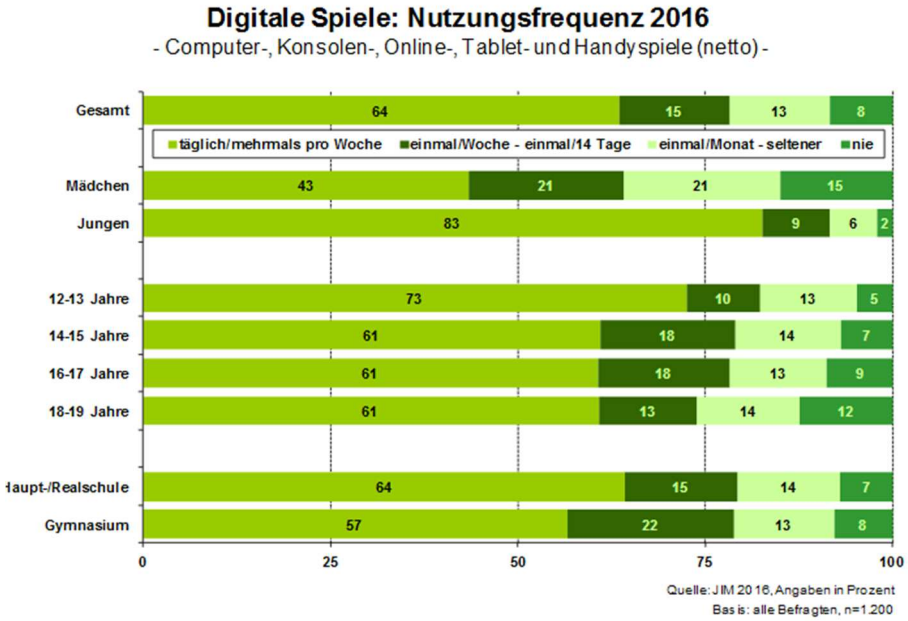
Hinsichtlich der Internetnutzung sticht die Kommunikation hervor. 41% der Online-Nutzung werden für kommunikative Aspekte aufgewendet, knapp 30% entfallen auf die Unterhaltung. An dritter Stelle sind die Spiele, deren Prozentsatz mit zunehmenden Alter ein wenig abnimmt, hingegen der Prozentsatz der Informationssuche zunimmt.

**Inhaltliche Verteilung der Internetnutzung 2016**

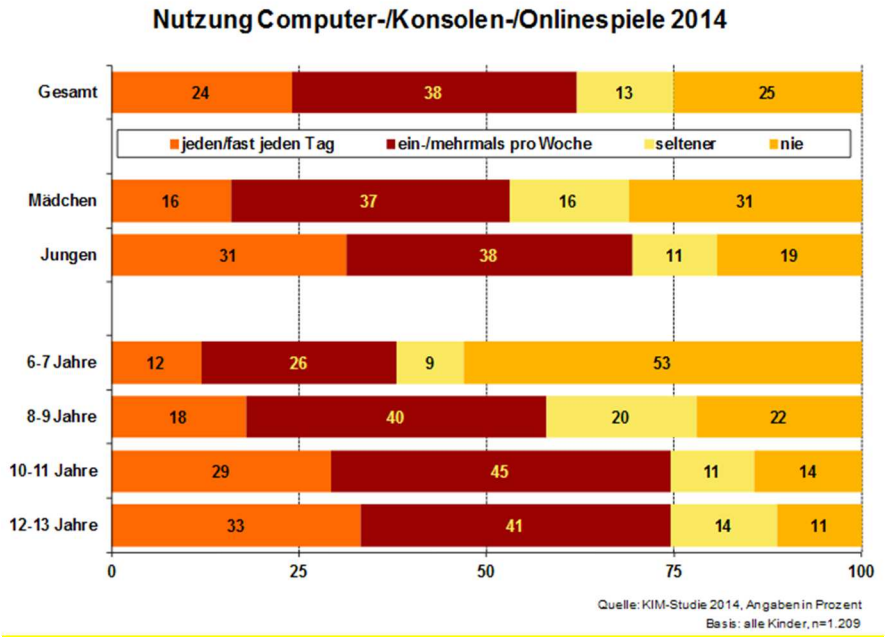



Quelle: JIM 2016, Angaben in Prozent
Basis: Internet-Nutzer, n=1.188

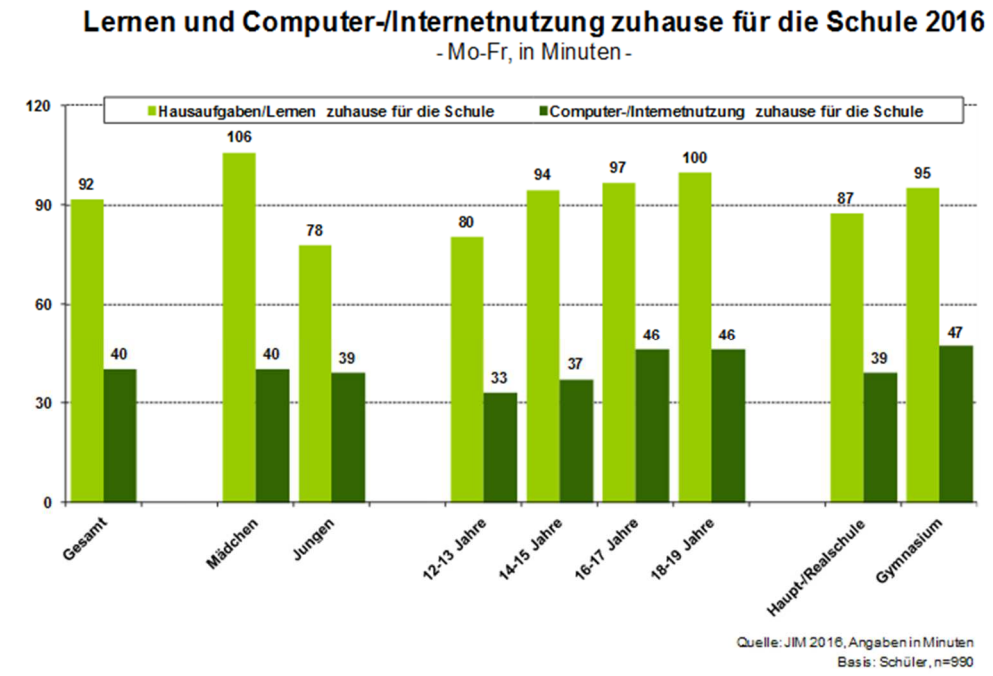
Da in den letzten Jahren den BEE SECURE Trainern aufgefallen ist, dass immer mehr Jugendliche spielen, ist ein Blick auf die Statistik bezüglich der Nutzungsfrequenz aus der JIM-Studie interessant. Im Juli 2016 gaben knapp Zweidrittel (64%) der 12- bis 19-Jährigen an, dass sie täglich oder mehrmals pro Woche spielen, unabhängig von der digitalen Spieloption (Computer, Konsole, Online, Tablet, Smartphone). Nach eigenen Angaben spielen nur acht Prozent der Befragten nie.




Auch vor dem Hintergrund der KIM-Studie 2014 fällt auf, dass Online-Spiele schon im Jahre 2014 sehr beliebt waren unter den jungen Menschen. 24% der Befragten gaben an, täglich oder fast jeden Tag zu spielen. Der Prozentsatz steigt von 12% bei den 6- bis 7-Jährigen auf 33% bei den 12- bis 13-Jährigen. 38% spielen ein- oder mehrmals pro Woche, wobei sich hier das gleiche Bild darstellt wie eben: 26% bei den 6- bis 7-Jährigen auf 41% bei den 12- bis 13-Jährigen. 53% der Jüngsten (6 bis 7 Jahre) spielen laut eigenen Angaben nie. Auch ist ein Unterschied zwischen den Geschlechtern sichtbar: Jungen spielen weitaus mehr als Mädchen. Aktuellere Zahlen gibt es leider nicht, jedoch ist auch hier ein Anstieg der Zahlen zu erwarten.




In Luxemburg greifen die Schüler beim Lernen gerne auf das Internet zurück. Die JIM-Studie 2016 zeigt, dass auch in Deutschland Jugendliche zwischen 12 und 19 Jahren täglich 40 Minuten am Computer oder im Internet verbringen um etwas für die Schule zu erledigen. Dieses entspricht fast der Hälfte der Zeit, die sie für Hausaufgaben aufbringen.




Insgesamt wird das Internet immer mehr in den Alltag integriert. Die Berichte der Trainer stimmen überein, dass die Menschen immer mehr auf Technologien zurückgreifen, diese jedoch nicht wirklich verstehen. Aus diesem Grund ist Aufklärung und Prävention ein wichtiger Schritt.

## Technischer Schutz

### Schadprogramme

Wenn der BEE SECURE Trainer in der Klasse fragt, wer schon einmal einen Virus oder einen Wurm auf seinem Gerät hatte, gibt es kaum ein Schüler der nicht aufzeigt. Es wird leider immer wieder festgestellt, dass Schüler die Schadsoftware als ein unausweichliches Übel hinnehmen, obwohl sie genau wissen, dass es Viren, Würmer und Trojaner gibt. Doch statt sich mit dem präventiven Schutz des Computers zu befassen, werden Warnungen und Fehlermeldungen oft solange ignoriert, bis ein Schaden das Gerät unbenutzbar macht.

Bezüglich Schadsoftware wissen Schüler viel zu berichten. Einige erzählen, dass sie sich auf illegalen Seiten ein Virus eingefangen haben, andere haben die Datei einer zwielichtigen E-Mail geöffnet und sich so einen Trojaner installiert, der anschließend Daten vom Computer gelöscht hat. Eine Schülerin berichtete, dass sie von einer Freundin eine private Nachricht auf Facebook zugesandt bekam, in der die Freundin auf Englisch von ihrem letzten Urlaub erzählte und ihr einen Link mitschickte auf dem sie sich die Fotos des Urlaubs anschauen könnte. Die Schülerin war aber skeptisch, da ihre Freundin ihr noch nie auf Englisch geschrieben hatte und auch nicht vor kurzem im Urlaub war, was sie wahrscheinlich vor einem Trojaner schützte. Bei einem weiteren Fall, hatte der Freund eines Schülers sich einen Trojaner heruntergeladen, der die Kamera dann fernsteuerte.

Auch die Smartphones bleiben nicht von Schadprogrammen verschont. Mehrere Apps zeigen Benachrichtigungen, dass angeblich ein Virus auf dem Smartphone gefunden wurde. Diesbezüglich fragen Schüler in der Schulung nach, ob sie dieser Benachrichtigung Glauben schenken sollen oder lieber nicht. Eine Schülerin erzählte, dass sie einmal eine Handyrechnung von einigen Hundert Euro durch eine Schadsoftware auf ihrem Smartphone hatte.

Kostenlose Webinhalte wie Spiele oder Apps, Musik- und Filmdownloads sind sehr beliebt bei Jugendlichen. Dass sich auf solchen Seiten viele Viren verstecken, macht ihnen keine Sorgen. Obwohl viele berichten, dass sie sich beim Filesharing schon Schadsoftware heruntergeladen haben, ist das für die Wenigstens ein Grund mit den Downloads aufzuhören. Dementsprechend versucht der BEE SECURE Trainer den Schülern diese Gefahr bewusst zu machen.

In manchen Klassen berichteten, vorwiegend Jungen, ganz stolz, dass sie ihr Smartphone „gejailbreaked“ haben. Beim „Jailbreak“ (benutzt bei iOS-Geräten) oder beim „Rooten“ (benutzt bei Android-Geräten) handelt es sich um das Entfernen von Nutzungsbeschränkungen auf einem Smartphone. So können auch nicht-autorisierte Apps auf dem Smartphone installiert und genutzt werden. Selten ist den Schülern bewusst, dass sie damit wichtige Sicherheitsmechanismen löschen und so Schadsoftware leichter angreifen kann.

### Schutzmaßnahmen

Aus der allgemeinen Sorglosigkeit gegenüber Schadprogrammen resultiert ein entsprechend nachlässiger Umgang mit den verschiedenen technischen Schutzmaßnahmen. In der BEE SECURE Schulung wird daher im Bereich der Schutzmaßnahmen der Fokus auf Antivirenprogramme und die Firewall, sowie das regelmäßige Aktualisieren (Update) aller Programme und das regelmäßige Speichern von Dateien

(Backup) gelegt. Entgegen dem Glauben der meisten Schüler, reicht es nicht aus, dass ein Antivirusprogramm nur auf dem Gerät installiert ist, sondern gerade dieses muss regelmäßig aktualisiert werden um auf aktuellem Stand zu sein und somit zuverlässig zu arbeiten. Warnhinweise, die automatisch erscheinen, wenn für ein Programm eine Aktualisierung zur Verfügung steht, werden von den Jugendlichen oft als störend und nicht dringend wahrgenommen und somit wird das „nervige Pop-Up" einfach nur schnell weg geklickt. Die BEE SECURE Trainer merken auch immer wieder, dass bei den Grundschülern keiner ein Antivirusprogramm auf dem Smartphone hat, in der Sekundarschule sind es nur 3-4 Schüler pro Klasse. Daher appellieren sie an die Schüler, dass auch Smartphones anfällig sind für Viren und dadurch mit einem Antivirusprogramm ausgestattet sein sollten. Auch die Eltern sollten sich bewusst sein, dass ein Schadprogramm einen großen Schaden bei ihren Kindern anrichten kann oder auch den Ruf ihres minderjährigen Opfers in Mitleidenschaft ziehen kann. Dies bspw. durch einen Spam-Trojaner, Passwort-Hacking und daraus resultierende Verleumdung oder das Ausnutzen des Computers durch Dritte für kriminelle Aktivitäten.

Erwähnenswert ist auch, dass es kostenlose und kostenpflichtige (meistens vorinstalliert) Antivirenprogramme gibt. Schüler mussten leider schon erfahren, dass man sich ein Virus einfangen kann, wenn man ein solches Programm von einer falschen Seite herunterlädt. Deshalb sollte bei der Installation des Antivirenprogrammes darauf geachtet werden.

Während den Schulungen bei den Jugendlichen sowie auch bei den Erwachsenen, stellen die Trainer immer wieder fest, dass es große Wissenslücken bezüglich der technischen Aspekte in der Informationssicherheit gibt, wie bspw. bei der Funktionsweise der Firewall sowie auch wie und warum man Backups seiner Dateien durchführen sollte.

Seit September 2014 setzt BEE SECURE im Bereich der Schutzmaßnahmen auf das Konzept #BeeFirstAid. Bei Veranstaltungen oder in Jugendhäusern werden die Smartphones der Jugendlichen in deren Beisein auf Sicherheitslücken untersucht und es werden einfache Tricks zum Datenschutz gezeigt. Diese Aktivität findet sehr viel Anklang.

Jugendliche sind nach wie vor sehr nachlässig mit ihren Passwörtern. Meistens kennen sie zwar die Basisregeln für ein gutes Passwort (mindestens 12 Zeichen; Groß- und Kleinbuchstaben, Zahlen und Sonderzeichen), jedoch entscheiden sie sich oft für eine einfache Zahlenkombination wie das eigene Geburtsdatum oder ihren Namen. Ein Schüler erzählte einem Trainer, dass er als Passwort „Passwort" benutze, da er sich das leicht merken könnte – und dies ist kein Einzelfall. Zusätzlich benutzen die Jugendlichen meistens überall das gleiche Passwort. So ist es natürlich für andere sehr einfach sich in alle Konten wie bspw. E-Mail oder Facebook anzumelden.

Des Weiteren geben Jugendliche ihr Passwort im Vertrauen an Freunde weiter. Wenn die Freundschaft zerbricht oder die Beziehung vorbei ist, kann dieses zum Problem werden. Ein Schüler berichtete, dass er seinem besten Freund sein Facebook-Passwort gegeben hatte. In einer Streit-Situation meldete sich der beste Freund im Profil des anderen an und verbreitete Lügen und bösartige Kommentare. Daraufhin redete niemand mehr mit dem Schüler, dessen Facebook-Konto missbraucht wurde, da jeder glaubte er selber hätte die Kommentare online gestellt. Dies zeigt, dass das virtuelle Leben sehr schnell aus dem

Ruder laufen kann, wenn Passwörter weitergegeben werden. Deshalb bemühen sich die BEE SECURE Trainer, den Jugendlichen zu vermitteln, wie wichtig ein gutes Passwort ist und, dass man es für sich behalten soll. Nur den sehr jungen Schülern wird empfohlen, das Passwort mit den Eltern zuteilen, für den Fall, dass sie es vergessen sollten.

## Soziale Netzwerke, Chat und E-Mail

Die Jugendlichen nutzen das Internet vor allem um mit ihren Freunden in Kontakt zu bleiben. Deshalb ist es nicht verwunderlich, dass soziale Netzwerke und Chats unter ihnen sehr beliebt sind. Jedoch lauern aber auch genau in diesen viele Gefahren, denen sich die Jugendlichen selten bewusst sind.

### Nutzung

Die sozialen Netzwerke bieten den Jugendlichen eine Plattform zur Selbstdarstellung. Jeder hat die Möglichkeit sich nach außen so zu zeigen, wie er wahrgenommen werden will. Unter den Jugendlichen herrscht ein großer Druck möglichst cool (hauptsächlich bei den Jungen) oder begehrenswert (hauptsächlich bei den Mädchen) zu wirken. Durch zeitnahe Bewertungen, wie bspw. bei Facebook mit „Likes“, bekommen sie direkte Rückmeldung. In manchen Fällen, können Beiträge aber auch zu scharfer Kritik oder gar Beleidigungen führen, welche das Selbstbewusstsein der Person stark beschädigen können. Daher ist eine verantwortungsbewusste Medienerziehung notwendig. Unter anderem auch, da die meisten Jugendliche mehr als nur ein soziales Netzwerk nutzen.

Facebook galt lange Zeit als das „must have“ unter den Jugendlichen. Jedoch stellen die Trainer in den letzten Jahren immer öfters fest, dass Facebook nicht mehr als das beliebteste soziale Netzwerk bei Jugendlichen in Luxemburg gilt. Eine Vermutung wieso es zu diesem Rückgang kam, ist, dass mittlerweile auch viele Erwachsene dieses soziale Netzwerk nutzen und es somit als „uncool“ angesehen wird, das gleiche Netzwerk wie bspw. die Eltern zu benutzen.

Vor allem Snapchat, Instagram oder Viber gewannen in den letzten Jahren an Beliebtheit. Viele Grundschulkinder haben bereits ein Snapchat oder Viber-Konto. Es fällt auch auf, dass die meisten Jugendlichen eher Viber benutzen um untereinander zu kommunizieren, hingegen WhatsApp als Kommunikationsmittel mit den Eltern gebraucht wird. Twitter wird eher von Jungen benutzt, um Gamern zu folgen und so immer, was Online-Spiele betrifft, auf dem neuesten Stand zu sein. Youtube bleibt weiterhin beliebt bei allen Jugendlichen.

Kurzweilig waren die Netzwerke musical.ly (Karaoke-App), younow (kostenlose Live-Videostreaming-Plattform) und ask.fm („Ask and answer. Find out what people want to know about you!”, Möglichkeit anderen Personen anonym eine Frage zu stellen) auch im Trend. Gegen Ende des Schuljahrs 2015/2016 wurden diese aber nur noch selten in den Schulklassen erwähnt.

Darüber hinaus, hängt die Anzahl der Jugendlichen die das jeweilige soziale Netzwerk benutzen aber auch von der Region des Landes ab. So werden in der Hauptstadt soziale Netzwerke häufiger und auch früher benutzt als in den ländlichen Gebieten.

BEE SECURE hat im Jahre 2016 auf 2 Veranstaltungen junge Menschen zwischen 11 und 30 Jahre befragt, welche sozialen Netzwerke sie benutzen. 93,1% der 11-15-Jährigen und 91,4% der 15-30-Jährigen haben

„Youtube“ angegeben, das sich somit als das meistgenutzte soziale Netzwerk absetzt. Bei den 11-15-Jährigen belegt Platz zwei „Snapchat“ (91,7% der Befragten), auf Platz drei folgt „Instagram“ (80,6%) und erst auf Platz vier ist „Facebook“ (79,2%) zu finden. Bei den 15-30-Jährigen verteilen sich die Plätze anders: Platz zwei belegt „Facebook“ (86,9%), gefolgt von „Snapchat“ (81,7%) und „WhatsApp“ (73,1%; WhatsApp wird nur von 50% der 11-15-Jährigen benutzt). Erst an fünfter Stelle tritt „Instagram“ (69,1%) auf.

Da schon viele Grundschüler in den sozialen Netzwerken aktiv sind, berichteten in den vergangenen Jahren verschiedene Grundschullehrer, dass sie diese aktiv in den Schulalltag integrieren. So können sich Schüler bspw. über die Hausaufgaben in einer Facebook-Gruppe austauschen.

E-Mail hat als Kommunikationsmittel unter den Jugendlichen ausgedient. Nur noch größere Anhänge (z.B.: Gruppenarbeiten in der Schule) werden per E-Mail versendet. Es kommt öfters vor, dass die Jugendlichen eigentlich nur eine private E-Mail-Adresse (jeder Schüler hat eine E-Mail-Adresse von der Schule) haben, um sich bei sozialen Netzwerken anzumelden und somit nicht mal mehr das Passwort zu dem Konto wissen.

## Gefahren

Im Allgemeinen scheint es den BEE SECURE Trainern, dass die Schüler mehr auf die Privatsphäre-Einstellungen achten. Ein Grund könnten die vielen Negativbeispiele sein. Jedoch beschweren sich Schüler aber auch immer wieder wie undurchsichtig Facebook ist und, dass die Privatsphäre-Einstellungen dort schwer verständlich sind. Dennoch reichen nur gute Privatsphäre-Einstellungen nicht aus um den Gefahren in sozialen Netzwerken adäquat zu begegnen.

So stellt bspw. die Freundesliste in sozialen Netzwerken eine Gefahr dar, die Jugendliche oft unterschätzen. Laut Schülern gilt die Anzahl der Freunde als Statussymbol: Je mehr Freunde man hat, desto beliebter ist man. Daher werden oft Fremde als Freunde akzeptiert und erhalten somit Einblicke in die Privatsphäre der Jugendlichen. Die Frage, ob diese unbekannten Personen alles wahrheitsgetreu angegeben haben, stellen sich die meisten nicht. Somit könnte bspw. ein 50-jähriger Mann hinter einem Facebook-Profil eines 13-jährigen Mädchens stecken oder umgedreht, ein 15-jähriger Junge könnte sich als 30-jährige Frau ausgeben. So genannte Fake-Profile sind einfach zu erstellen und kommen häufiger vor als gedacht. 2014 rechnete Facebook mit 5-11% Fake-Nutzern und Duplikaten[4]. In den Grundschulen geben viele Schüler an, dass sie mindestens bei der Altersangabe geschwindelt haben um Facebook überhaupt benutzen zu können (Facebook ist erst ab 13 Jahren erlaubt). Jedoch werden auch solche gefälschten Profilseiten mit dem Ziel erstellt, andere auszuspionieren und dabei selbst unerkannt zu bleiben oder im Namen eines anderen Unfug zu treiben. Des Öfteren berichten Schüler, dass sie mehr als 1000 Freunde haben, die sie wiederum nicht alle selbst kennen und sich dann später wundern, dass ihre Fotos auf anderen Profilen oder sozialen Netzwerken zu sehen sind. Auch gab es schon Schüler, die ein Fake-Profil angelegt haben um unauffällig mit dem Lehrer in Kontakt zu kommen. Bei einem Vorfall, ging es soweit, dass der Lehrer, der Frau (hinter der sich die Schüler versteckten) ein Nacktbild zugesandt hatte,

[4] http://thenextweb.com/facebook/2014/02/03/facebook-estimates-5-5-11-2-accounts-fake/

dieses kurz darauf in der Schule kursierte und zur Suspendierung des Lehrers führte. Über die rechtlichen Konsequenzen ihrer Online-Aktivitäten machen sich die Schüler eher selten Gedanken.

Im Zusammenhang mit den Fake-Profilen besteht auch die Gefahr der privaten Treffen. Schüler vertrauen der unbekannten Person und sehen einem privaten Treffen sorgenfrei entgegen. Jedoch kann dort eine komplett andere Person auftauchen als erwartet. Manche Schüler erzählen von solchen Treffen in der BEE SECURE Schulung. In den meisten Fällen, ist dann wirklich die erwartete Person aufgetaucht, jedoch schilderte auch ein Schüler, dass er sich einmal mit einem Jungen in einem großen Einkaufszentrum treffen wollte. Am vereinbarten Treffpunkt angekommen, wartete er eine halbe Stunde auf den anderen, jedoch kam keiner. Während der ganzen Zeit fühlte er sich aber von einem älteren Mann beobachtet. Wieder zu Hause angekommen, vertraute er sich seinen Eltern an und brach den Kontakt mit der Person sofort ab. Die BEE SECURE Trainer appellieren deshalb immer, dass man sich nicht mit Freunden, die man nur aus der virtuellen Welt kennt, treffen sollte. Falls dieses jedoch unbedingt erwünscht ist, dann nur in Begleitung eines Erwachsenen und an einem belebten Ort. Zudem werden Jugendliche in der Schulung dazu aufgefordert suspekte „Freunde“ zu melden, die „Freundschaft“ sofort zu beenden und mit einer Vertrauensperson über unangenehme Situationen im Internet zu sprechen.

Schüler sind sich auch nicht immer bewusst, dass Falschmeldungen in sozialen Netzwerken kursieren. Viele beißen bei auch noch so absurden Meldungen an, teilen sie oder klicken auf fingierte Links.

Während der BEE SECURE Schulung erwähnen die Trainer öfters den Satz „einmal im Netz – immer im Netz“. Damit wollen sie darauf eingehen, dass die Schüler sich gut überlegen sollen was sie ins Netz stellen, da das Internet nichts vergisst. Die meisten Schüler sind erstaunt, wenn sie vom Trainer hören, dass alle sozialen Netzwerke jeden Schritt von jeder Person speichern. Erst dann verstehen sie, dass auch wenn sie ein Foto gelöscht haben, es noch immer auf dem Server der jeweiligen Firma gespeichert bleibt. Viele Schüler reagieren schockiert darauf und ihnen wird bewusst, dass das Internet gar nicht so privat ist. Auch können in der Zeit wo bspw. ein Foto online ist, andere Personen dieses speichern oder ein Bildschirmfoto machen. In den letzten Jahren gab es mehrere Fälle, wo gelöscht-geglaubte Fotos wiederaufgetaucht sind. So hatte ein Mädchen ein relativ freizügiges Foto auf Facebook gestellt. Nach 10 Minuten wurde ihr bewusst, welche Dummheit sie gemacht hatte und löschte das Foto unverzüglich. Am darauf folgenden Tag wurde sie in der Schule öfters darauf angesprochen und im Klassenraum hing dieses Foto auf der Pinnwand. Irgendjemand hatte das Foto in den 10 Minuten wo es online war gespeichert und verbreitet. Ein weiterer Fall betraf 3 Jungen auf Snapchat. Diese hatten über dieses soziale Netzwerk Fotos von ihren Genitalien ausgetauscht. Einer von den Dreien hat während dem Countdown ein Bildschirmfoto gemacht und es in der Schule verbreitet. Meistens erwähnen Schüler während der Schulung weitere Beispiele und schildern, dass solche Fotos zu Cybermobbing führen können. Mehr zu Cybermobbing in einem späteren Kapitel.

Ferner können die sozialen Netzwerke, vor allem Facebook, auch als eine Art „Rache-Plattform“ genutzt werden. 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 öffentliches Foto im weltweiten Netz publiziert ist und auch nach dem Löschen unverhofft wiederauftauchen kann.

Es ist weiterhin erstaunlich wie blauäugig Schüler Privatadresse, Handynummer und weitere Kontaktdaten (z.B. Geburtsdatum, Angabe der Schule) oder auch anzügliche Fotos in sozialen Netzwerken veröffentlichen. Dieses kann natürlich dazu führen, dass sie von Fremden belästigt oder gar im schlimmsten Fall auch im realen Leben verfolgt werden können. BEE SECURE Trainer berichten zudem auch, dass gefühlsmäßig die Anzahl der Jugendlichen die in sozialen Netzwerken und Chats mit sexueller Belästigung konfrontiert werden, in den letzten Jahren gestiegen ist. Immer wieder werden vor allem Mädchen dazu aufgefordert, sich vor der Kamera auszuziehen oder Nacktfotos zu senden.

Wie schon im vorherigen Kapitel erwähnt, besteht eine weitere Gefahr in den sozialen Netzwerken durch das Wählen eines leicht zu erratenden Passwortes oder die Weitergabe von diesem. Zahlreiche Berichte von Schülern belegen, dass sich vermehrt Außenstehende in Profilen von anderen anmelden und in dessen Namen beleidigende Kommentare oder Gerüchte veröffentlichen.

Zum Thema „Gefahren in sozialen Netzwerken“ wurde in den letzten beiden Schuljahren der „Facebook Check“ verteilt. Der Flyer im Smartphone-Format wurde von Jugendlichen des „BEE SECURE Youth Panels“ entwickelt und dokumentiert auf lustige Weise die wichtigsten Verhaltensregeln im sozialen Netzwerk.

E-Mail-Adressen werden von den Jugendlichen großzügig weitergegeben. Folglich erhalten sie große Mengen an Spam sowie Ketten-E-Mails und dubiose Nachrichten von unbekannten Absendern. Wobei Ketten-E-Mails nicht zu unterschätzen sind, denn auch wenn sie vermeintlich harmlos wirken, können sie gefährlich werden. Oft tauchen sie in Wellen auf und werden durch neue ersetzt sobald der „Hype“ der Nachricht nachlässt. Viele Ketten-E-Mails warnen vor vermeintlichen Gefahren wie Geister, Viren oder Gebühren für die Nutzung eines Services, andere schüren Hass oder verbreiten Gerüchte. Bedrohlich sind Kettenbriefe, die mit vermeintlichen Gutscheinen dazu locken auf Links, die zu einer Schadsoftware führen, zu klicken oder aber mit Horror-Stories besonders Kinder einschüchtern oder verängstigen, denn diese haben oft Schwierigkeiten, die Botschaften richtig einzuordnen. Auch wenn die Ängste, die in den Kettenbriefen geschürt werden, irrational sind, so sind die Sorgen und Ängste der Kinder durchaus real. Es ist daher wichtig, dass Eltern und Erzieher den Kindern erklären, dass diese vermeintlichen Gefahren erfunden sind und mit ihnen über die verschiedenen Arten von Kettenbriefen diskutieren.

Erwähnenswert ist auch das Urheberrecht. Die meisten Schüler wissen zwar von ihren Lehrern, dass sie nicht einfach Bilder oder Texte aus dem Internet kopieren dürfen, ohne diese als Zitate zu kennzeichnen und mit Quellennachweisen zu vermerken, jedoch außerhalb der Schule ist dieses oft vergessen. Viele Schüler laden sich Filme und Musik von häufig dubiosen Seiten im Internet herunter. Neben der Gefahr, dass sie sich ein Schadprogramm herunterladen, sehen sie nicht ein, dass sie die Künstler um einen Teil ihres Verdienstes betrügen und haben auch vor einer eventuellen gerichtlichen Verfolgung keine Angst. Nur ein relativ kleiner Teil von Schülern lädt solche Inhalte legal auf vertrauenswürdigen Seiten herunter und bezahlt dafür. Es handelt sich hierbei meist um Kinder, deren Eltern die Thematik mit ihnen besprochen haben, und das Geld für das legale Herunterladen zur Verfügung stellen.

## Cybermobbing

Cybermobbing ist und bleibt ein aktuelles Thema. „NOT FUNNY – BEE FAIR“, die Kampagne, die sich mit dem Kampf gegen Cybermobbing befasste, wird in jeder Schulung wieder aufgegriffen. Auch wenn die

Anzahl der Anrufe zu Cybermobbing bei der BEE SECURE Helpline nur geringfügig anwächst, so vermerken die Trainer in den Schulen einen hohen Anstieg von Cybermobbing.

Das Thema ist bei den Jugendlichen von großem Interesse, vor allem, da sie sich meistens damit identifizieren können. Viele kennen bereits Fälle, sei es nun als Zeuge oder aus den Medien. Häufig wird in den Schulungen der Fall von Amanda Todd erwähnt, ein 16-jähriges Mädchen aus Kanada, die sich wegen Cybermobbing umbrachte. Ihr Fall wurde bekannt, da sie vor ihrem Suizid ein neunminütiges Video, in dem sie stumm auf handgeschriebenen Zetteln ihre Geschichte offenbart, auf Youtube veröffentlichte. In manchen Klassen sind auch Mobbing-Opfer, die von ihren Erlebnissen berichten. Gegenüber den Trainern zeigen sich die Schüler meist schockiert über Mobbing und solidarisch mit dem Opfer, vor allem wenn das Opfer als einzige Flucht Selbstmord sah. Die rechtlichen Konsequenzen sind den Schülern selten bekannt.

Übergreifend berichten Schüler von Hass-Gruppen gegen eine bestimme Person auf Facebook, Drohungen und Erpressungen über Nachrichten, veröffentlichte Beleidigungen, peinliche Fotos und Videos, verbreitete Gerüchte usw. Mit Erschrecken stellen die Trainer aber auch fest, dass sie immer öfters schon bereits im Cycle 3 der Grundschule mit (Cyber-)Mobbing konfrontiert werden. So gab es in einer Klasse einen solchen Fall über Sprachnachrichten. In einer anderen Klasse sprachen die Schüler Suizid an, da sie Fälle aus dem Bekanntenkreis kannten und zudem auch Schüler aus der Maison Relais sich wegen Mobbing ritzten. In einer anderen Schule, fingen 3 Schüler aus dem Cycle 4 an zu weinen und brachen zusammen als der Trainer über Cybermobbing sprach. Später stellte sich heraus, dass diese Schüler wegen Cybermobbing umgezogen sind und die Schule gewechselt hatten. Ein Achtklässler erzählt in der Schulung, dass ein Mädchen aus Luxemburg sich umgebracht hat, da sie als „dickes Mädchen“ beschimpft wurde. Auch die Berichte der höheren Klassen zeigen, dass Cybermobbing altersunabhängig ist.

Des Weiteren ist den Schülern der Unterschied zwischen Mobbing und Cybermobbing oft bekannt. Durch Smartphones und das Internet sind Cybermobbing-Opfer den Attacken 24 Stunden am Tag während 7 Tagen die Woche ausgeliefert. Jedes Mal, wenn das Smartphone klingelt, eine Benachrichtigung bei Facebook aufleuchtet oder der Posteingang eine neue E-Mail ankündigt, erstarren die Opfer vor Panik. So kann man dem Täter nicht entfliehen, bei Mobbing in der realen Welt ist dies eher möglich. Dazu kommt, dass Situationen bei Cybermobbing schnell außer Kontrolle geraten können. Deshalb werden Schüler, wie bereits erwähnt, auf „einmal im Netz – immer im Netz“ aufmerksam gemacht. Denn auch wenn ein Foto nur versehentlich hochgeladen worden ist, kann es schnell in Umlauf kommen und die ganze Welt kann daran teilhaben. Dadurch vergrößert sich oftmals auch der Kreis der Täter.

Es gibt keine bestimmte Tendenz ob sich Schüler im Fall von Mobbing eher dem Lehrpersonal anvertrauen oder ihren Eltern. Dieses hängt wahrscheinlich vom Alter der Schüler, von der Härte des Mobbings und vom Verhältnis zu den Eltern ab. In der Schulung gehen die Trainer darauf ein, wie wichtig es ist, sich einer möglichst erwachsenen Person anzuvertrauen und bewerben in dem Zusammenhang die BEE SECURE Helpline (8002 1234).

Die Rolle der BEE SECURE Trainer ist es, den potentiellen Opfern die wichtigsten Grundregeln im Umgang mit verletzenden Nachrichten oder Fotos, sowie den Zeugen die Wichtigkeit des Nicht-Wegsehens zu

vermitteln. Zudem verweisen sie auf die bestehenden Anlaufstellen (Eltern, SPOS, Lehrer/Erzieher, BEE SECURE Helpline, …).

Leider kann BEE SECURE das Auftreten von Cybermobbing nicht verhindern, aber die Tatsache, dass in den Schulungen offen darüber berichtet wird und auch die BEE SECURE Helpline verstärkt von Betroffenen genutzt wird, spricht für ein erweitertes Bewusstsein dafür, dass über derartige Themen auf keinen Fall geschwiegen werden darf.

## Sexting

Der Begriff „Sexting“ setzt sich aus den Wörtern „Sex“ und „Texting“ zusammen. Er beschreibt das Austauschen intimer Nachrichten bzw. Fotos über Smartphones und soziale Netzwerke. Die größte Gefahr beim Sexting sind Nacktaufnahmen, die als privater Vertrauensbeweis gedacht waren und plötzlich öffentlich im Netz zirkulieren.

Die Beweggründe, sich nackt zu fotografieren und das Foto dann weiter zu schicken, sind vielfältig. Häufig entstehen die intimen Fotos im Rahmen einer Liebesbeziehung. Nach dem Scheitern der Liebesbeziehung bringen dann die Ex-Partner oder ehemals beste Freunde die Fotos in Umlauf, um bewusst der anderen Person weh zu tun und ihr zu schaden. Worüber sie sich selten bewusst sind, ist, dass diese kurze Schadenfreude oder die Rache, für den anderen traumatische Erfahrungen mit sich bringen können, die sie im schlimmsten Fall ein Leben lang begleiten. Andere wiederum stellen ihren eigenen Körper selbstbewusst zur Schau und erhoffen sich damit Anerkennung, was jedoch nicht immer der Fall ist. Vor allem bei jungen Mädchen kommt es vor, dass sie von ihrem Freund dazu gedrängt werden, Nacktfotos zu machen, oder sich freizügig filmen zu lassen.

Sexting ist ein Phänomen, das vor allem unter Jugendlichen und jungen Erwachsenen verbreitet ist, aber auch schon im Cycle 4 der Grundschule auftaucht. Der Fall von den 3 Jungen, die über Snapchat Fotos von ihren Genitalien ausgetauscht hatten, war zum Beispiel ein Fall aus der Grundschule.

Im Zusammenhang mit Sexting wird öfters die App „Snapchat“ gebracht, die mancherorts sogar als „Sexting-App“ bezeichnet wird. Bei Snapchat scheint es so, dass die Fotos nur für eine vorher eingestellte Zeitspanne (maximal 10 Sekunden) sichtbar sind und anschließend sofort gelöscht werden. Dieses verleitet natürlich vor allem Jugendliche freizügige Fotos über diese App zu verschicken, da sie annehmen, dass das Fotos nach dem Betrachten für immer gelöscht sei. Dass sich solche Fotos trotzdem speichern lassen, hat sich jedoch schon bestätigt. Die Aufnahmen können nämlich über Apps von Drittanbietern gespeichert werden, oder einfach per Bildschirmfoto. Die BEE SECURE Trainer berichten, dass es aber den Anschein hat, dass sich die Schüler dessen heute bewusster sind als noch 2014 oder 2015.

In diesem Kontext wird auch auf pornografische Inhalte im Internet hingewiesen, da in der Regel alle Jugendlichen in der siebten Klasse bereits solche gesehen haben. Das betrifft gleichermaßen Jungen und Mädchen und reicht von Popups mit erotischem Inhalten bis hin zu Hardcore-Filmen. Problematisch ist, dass Kinder und Jugendliche, die meist noch keinerlei sexuelle Erfahrung haben, Inhalte konsumieren, die für ein erwachsenes und sexuell aktives Publikum geschaffen wurden.

Ein Unterschied ist bemerkbar in der Art und Weise, wie Pornografie von den Jugendlichen bewertet wird. Während Mädchen eher offen schockiert und angewidert reagieren, gehen Jungen ganz anders damit um. Das bedeutet aber nicht, dass sie nicht von den Inhalten überfordert wären. Jungen neigen auch eher dazu, regelmäßig Pornografie zu konsumieren und die anstößigen Filme in der Gruppe zu tauschen.

Eine gute Sexualerziehung sollte das Thema „Porno" nicht meiden, sondern offen darüber reden, da die Heranwachsenden früher oder später sowieso damit in Kontakt kommen. Nur so kann gesichert werden, dass Kinder in ihrer Entwicklung nicht negativ von Pornos beeinflusst werden und sie tatsächlich als inszenierte Filmszenen wahrnehmen.

### Recht am eigenen Bild

Welche Rechte bestehen auf eigenen Inhalt bzw. auf die eigene Privatsphäre im Internet? Diesbezüglich spricht der BEE SECURE Trainer in der Schulung das „Recht am eigenen Bild" an. Die meisten Jugendlichen sind sich nicht bewusst, dass sie eigentlich das Einverständnis benötigen um ein Foto von einer Person zu machen. Außerdem benötigen sie die Erlaubnis der abgebildeten Person, um das Foto ins Internet (z.B. auf Facebook) hochzuladen. Dieses wird zwar eher selten von Jugendlichen angewendet, jedoch sollen sie sich bewusst sein, dass es dieses Recht gibt und in Zukunft umsichtiger handeln.

Daher klärt der Trainer die Schüler darüber auf, dass sie eigentlich selber entscheiden dürfen, welche privaten Daten von ihnen veröffentlicht werden bzw. welche Handlungsmöglichkeiten bestehen, um im Streitfall ihr Recht einzufordern.

In einigen Fällen haben sich Schüler in den Klassen darüber beschwert, dass ihre Eltern Fotos von ihnen online stellen, ohne ihre Erlaubnis und obwohl die Schüler dagegen sind. Es ist ein kritisches Thema, in welchen Fällen das Recht des Kindes auch wirklich eingehalten werden sollte.

## Kampagne 2014/2015: Clever klicken

Mit der Kampagne „Clever klicken – Online-Betrug kann teuer werden" im Schuljahr 2014/2015, wollte BEE SECURE die Jugendlichen darauf aufmerksam machen online nicht blind auf alles zu klicken, sondern als erstes zu überlegen. Cyber-Kriminelle finden immer neue Strategien, bspw. ködern ihre Opfer über interessante Links zu Schadprogrammen oder täuschen falsche Gewinne vor. Durch die menschlichen Eigenschaften wie bspw. Neugierde, Mitleid oder Profitgier fallen die Jugendlichen aber auch die Erwachsenen auf solche Maschen herein. Schüler berichteten in den Schulungen von E-Mails in denen sie Hunderte von Euros gewonnen hätten oder auch von Pop-Ups, die ihnen das neueste iPad oder iPhone versprechen. Die BEE SECURE Trainer appellieren an die Schüler immer nachzudenken, ob es dieses auch im realen Leben geben würde. Falls sie diese Frage mit „nein" beantworten würden, sollten sie auch „clever klicken" und eben nicht auf solche Verlockungen klicken. Des Weiteren wird ihnen dazu geraten sich alles genau durchzulesen bevor man zum Beispiel an einem Gewinnspiel oder Quiz teilnimmt. Durch „Clever klicken" wird auch die Gefahr verringert, sich einen Trojaner durch gefälschte E-Mails herunterzuladen.

Auch bei der BEE SECURE Helpline kamen in den letzten Jahren vermehrt Anrufe zu Phishing (Nutzer werden getäuscht und dazu verleitet persönliche und vertrauliche Daten preiszugeben), Microsoft Scam

(Anrufe von angeblichen Microsoft-Mitarbeitern, die angeben, dass der Computer mit Schadprogrammen infiziert wäre oder, dass die Lizenzen nicht auf dem neuesten Stand wären) oder auch Ransomware (Erpressungssoftware, die die Daten verschlüsselt und somit unbrauchbar macht). Dies zeigt die Notwendigkeit des Themas.

## Kampagne 2015/2016: Clever Cloud User

Die Kampagne „Clever Cloud User. And you?“ zielte darauf ab, die Öffentlichkeit über die Cloud zu informieren. BEE SECURE Trainer stellten in den Schulen fest, dass die meisten Schüler der Sekundarstufe bspw. den Begriff „iCloud“ zwar kannten, jedoch nichts über die Technologie wussten und schon gar nicht, dass sie durch die Benutzung von Facebook und Co. auch eine sogenannte Cloud benutzen. Daher wurde dieser Begriff verständlich erklärt, die positiven Aspekte sowie auch die Risiken wurden vorgestellt und auch die rechtliche Situation dargelegt. Ein besonderer Fokus lag auf dem Schutz persönlicher Daten.

## Spiele

In den vergangenen Jahren ist den BEE SECURE Trainern aufgefallen, dass Spiele immer beliebter unter Kindern und Jugendlichen werden. Vor allem das Open-World-Spiel „Minecraft“, das Strategiespiel „Clash of Clans“, das Fußballspiel „FIFA“, aber auch gewaltvolle Spiele wie das Action-Game „Grand Theft Auto“, das First-Person-Shooter-Game „Call of Duty“ oder auch das Rollenspiel „World of Warcraft“ gehören zu den bevorzugten Spielen. Auch bei der JIM-Studie 2016 kam als Ergebnis, dass „FIFA“ (17%), „Minecraft“ (14%) und „Grand Theft Auto“ (9%), die 3 populärsten Spiele der 12-19-Jährigen sind. In Luxemburg stellen die Trainer fest, dass bereits im Cycle 2, mindestens 2-3 Kinder pro Klasse mehrmals wöchentlich spielen, wobei es sich meistens um „Minecraft“ oder „Grand Theft Auto“ handelt. Je älter die Schüler, desto gewaltvoller werden die Spiele.

Zudem nehmen die Trainer an, dass es bis zum Alter von 13/14 Jahren keinen Unterschied gibt, ob mehr Mädchen oder Jungen spielen, hingegen ab diesem Alter die Tendenz eher zu Jungen geht.

Neben der Gewalt in den Spielen kann auch die Spieldauer problematisch werden. Ein Schüler des Cycle 3.1 erzählte, dass er durchschnittlich am Wochenende etwa 20 Stunden spiele. Mit steigendem Alter nimmt die Anzahl der Schüler sowie auch die Stundenanzahl, in der die Schüler spielen, zu. Manche Lehrer geben an, dass verschiedene Schüler sogar vor der Schule schon spielen und solche Spiele bei einigen Schülern zu einer emotionalen Verlagerung beigetragen haben. Sie sind immer nervös oder werden schneller wütend und gewaltbereiter. Dementsprechend wird in der Schulung auf die BEE SECURE Kampagne „BEE balanced“ verwiesen, die ein Aufruf war, Computer, Smartphone und Co. in gesunden Maßen zu benutzen, so dass die Gefahr einer Abhängigkeitserscheinung oder emotionalen Gefühlsänderung geringer ist.

Über die Medien wurden auch schon Fälle bekannt, in denen Pädophile das Spiel Minecraft ausgenutzt haben um an Kinder und Jugendliche ranzukommen. Deshalb gilt auch bei den Spielen darauf zu achten, wer sich wirklich hinter dem anderen Spieler versteckt und kein Treffen mit Fremden stattfinden sollte.

## Die Rolle der Eltern

Für viele Eltern entwickelt sich die Technik zu schnell um mitzukommen. Häufig fehlt das nötige Know-how und auch der Wille, die Zeit oder die Möglichkeit es sich anzueignen. Die Kinder hingegen werden in diese Welt voller Technik hineingeboren. Als „Digital natives“ sind sie selbstbewusst im weltweiten Netz unterwegs, was meistens auf die Eltern sehr souverän wirkt. Dadurch bekommen viele Eltern die Auffassung „Mein Kind kennt sich eh besser mit Internet und Co. aus, also lass ich es mal machen”. 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. Viele scheinen das Gefühl zu haben, ohnehin nicht mit dem Tempo ihrer Kinder mithalten zu können.

Natürlich gibt es auch Eltern, die die neuen Medien viel nutzen. Das bedeutet aber längst nicht, dass es sich hierbei um eine (verantwortungs-)bewusste Nutzung handelt. Viele haben sich zwar mit der Funktionalität auseinandergesetzt, jedoch nicht mit den Risiken. Zudem halten sie sich, wie ihre Kinder auch, nicht auf dem Laufenden, was die Veränderungen im Bereich der Internetsicherheit angeht. Haben sie selbst bspw. ein Facebookkonto, so wird hier ebenso häufig sehr locker mit der An- oder Weitergabe persönlicher Informationen umgegangen. Auch in Bezug auf Privatsphäre-Einstellungen fehlt es bei einigen an Wissen und Bewusstsein. Dazu zählt auch, wie bereits erwähnt, dass manche Eltern, dem Wunsch ihrer Kinder, keine Fotos von Letzteren zu veröffentlichen, nicht nachkommen. Ebenso können Eltern ihren Kindern den Umgang mit den neuen Medien nicht verbieten, wenn sie selbst ständig das Smartphone in der Hand haben.

Häufig haben Eltern keine Zeit oder möchten sich keine Zeit nehmen um sich mit den Internetgewohnheiten ihrer Kinder auseinanderzusetzen. Das merken die BEE SECURE Trainer zum Beispiel, wenn sie Elternabende organisieren und nur wenige Anmeldungen erfolgen.

Die doppelte Viktimisierung ist ein weiteres Problem des Vertrauensverhältnisses zwischen den Eltern und ihren Kindern: Ein Kind wird bereits durch unfreiweillig konsumierte schockierende Inhalte zum Opfer. Falls dieses seine schlechten Erfahrungen seinen Eltern mitteilt, reagieren diese meist mit Entsetzen und wenig verständnisvoll. Häufig drohen Bestrafungen wie bspw. Internet-Entzug. Dies ist einer der Gründe, warum Kinder ungern mit ihren Eltern oder Erziehungsberechtigten über diese Art von Problemen reden.

Jedoch sollten Eltern die wichtigsten Vertrauenspersonen für ihre Kinder sein. Da 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 ein adäquater 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. Zudem werden Schulungen für die Eltern gemeinsam mit ihren Kindern (z.B. BEE Home Party) angeboten. Diese waren jedes Mal ein großer Erfolg und man möchte gerne an diesem Konzept feshalten.

2010 erschien erstmals die Elternbroschüre „Kuck mat wat deng Kanner maachen!“ in Zusammenarbeit mit luxemburgischen Experten aus den verschiedenen Bereichen der Internetsicherheit. Sie unterstützte Eltern in der Begleitung von Kindern und Jugendlichen durch die digitale Welt. Mitte 2016 erschien die bereits 4. Auflage der Broschüre als komplett überarbeitete Ausgabe, die die vielfältigen Themen noch ansprechender aufbereitet und zusätzliche Verweise auf das BEE SECURE Sensibiliserungsangebot enthält.

## Die Rolle der Lehrer

Obwohl Medienerziehung nicht als Fach im Schulplan verankert ist, sollten Lehrer trotzdem eine gewissenhafte Medienerziehung der Kinder anstreben. Doch bedauerlicherweise wird, wenn überhaupt, der richtige Umgang mit dem Smartphone, Internet und den anderen Medien in vielen Klassen nur am Rande behandelt.

In der Regel wird festgestellt, dass das Interesse der Lehrer an der BEE SECURE Schulung steigt. Viele Lehrer hören den Trainern aufmerksam zu und lernen laut eigenen Angaben selbst noch dazu. Andere, die sich mit Datenschutz und Informationssicherheit auskennen, bringen eigene Beispiele mit ein, die das Gesagte belegen. Manche Grundschullehrer nehmen sich viel Zeit um die Thematik mit ihren Schülern durchzuarbeiten und finden es gut, wenn die Schüler die wichtigsten Regeln noch einmal von „Experten“ hören. Diese Zeit können sich die Lehrer der Sekundarschule leider nicht nehmen. Engagierte Lehrer probieren dieses aber im „Tutorat“ anzusprechen.

Manche Lehrer erkennen auch erst durch die BEE SECURE Schulung die Notwendigkeit einer bewussten Medienerziehung. Die Trainer berichten, dass viele Lehrer nach der Schulung sich erstaunt zeigen, wie viel Zeit die Schüler mit den neuen Medien verbringen und wie gut bzw. schlecht sie sich damit auskennen. So gab es bspw. Fälle in Grundschulklassen, wo die Lehrer geschockt waren, dass fast die ganze Klasse „Minecraft“ oder „Grand Theft Auto“ spielen würde, obwohl sie selbst noch nie zuvor davon gehört hätten. In einer anderen Klasse hat der Lehrer erst in der Schulung erfahren, dass es einen Fall von Cybermobbing in seiner Klasse geben würde.

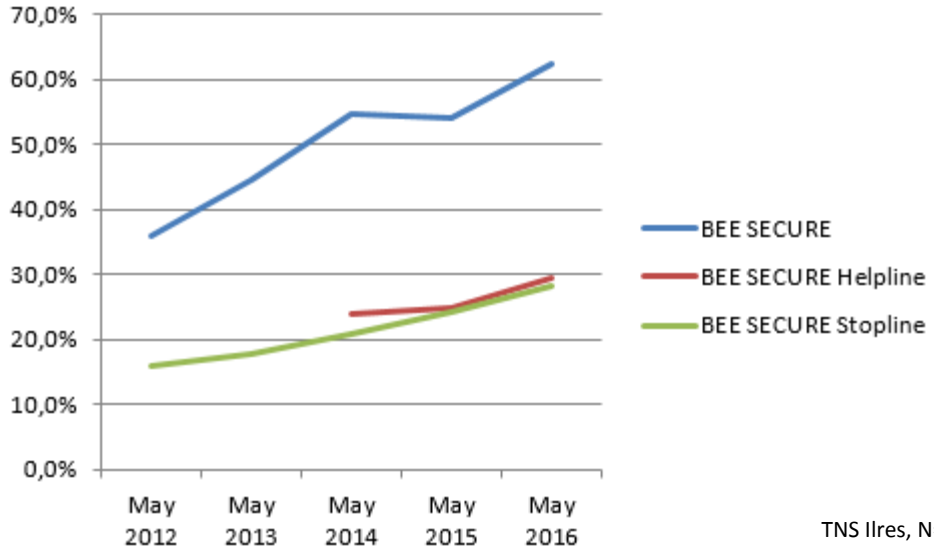
Leider können öfters Lehrer der älteren Generation die Wichtigkeit der Schulung nicht nachvollziehen, vor allem da sie meist wenig bis gar keinen Bezug zum Internet haben. Aufgrund des mangelnden Verständnisses wird die Notwendigkeit einer korrekten Medienerziehung angezweifelt.

Es wäre sehr wünschenswert, dass Medienkompetenz als Schulfach im Lehrplan verankert wäre. So könnte Computer- und Informationssicherheit ein fester Bestandteil der schulischen Ausbildung werden. Im Idealfall wäre Medienerziehung sogar 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 neuesten Stand zu halten. Dieses wäre denkbar durch regelmäßige (z.B. im Zweijahresrhythmus angebotene) pflichtmäßige Schulungen, an denen die Lehrer teilnehmen, damit sie ihren Schülern die entsprechenden Werte weiter vermitteln können.

## Ausblick

BEE SECURE hat in den letzten Jahren einen enormen Bekanntheitsgrad erlangt, wie die Studie von TNS ILRES, die jährlich seit 2012 durchgeführt wird, zeigt. Der Bekanntheitsgrad konnte sich in diesen 5 Jahren

fast verdoppeln von 36% auf 62,4%. Auch die Helpline und die Stopline erfahren einen kontinuierlichen Anstieg (die Bekanntheit der Helpline wurde ab 2014 unabhängig von BEE SECURE gemessen).




TNS Ilres, N=500, Age: 15-65 year olds

Auch im Schulumfeld lässt sich der steigende Bekanntheitsgrad beobachten. So berichten bspw. Schüler auf Veranstaltungen, dass sie bereits an einer BEE SECURE Schulung teilgenommen haben. Hinsichtlich der Schulungen, treffen die Trainer heutzutage in der Sekundarschule auf Kinder, deren Klasse sie bereits in der Grundschule besucht hatten. Häufig geben die Schüler an, dass sie viele Inhalte schon behandelt hätten. Jedoch merken die Trainer sowie auch die Schüler in der Schulung, dass einige Themen des damals Gelernten nicht ausreichend verinnerlicht wurden. Die Erfahrung zeigt, dass eine einzige Schulung von 90 Minuten nicht ausreicht, das Internetverhalten der jungen Menschen dauerhaft sicherer zu gestalten. Nur die Wiederholung des Gelernten und das konsequente Umsetzen in praktischen Übungen können ein Verinnerlichen der Sicherheitsratschläge fördern. Aus diesem Grund wünscht sich BEE SECURE die weitere **aktive Einbindung der Medienerziehung in den Unterricht** an den luxemburgischen Schulen sowie eine regelmäßige **Weiterbildung der Lehrkräfte** auf diesem Gebiet.

Die Trainer berichten immer wieder, dass 90 Minuten für die Schulung sehr kurz wären. Meistens beteiligen sich die Schüler sehr aktiv am Unterricht und teilen ihre Erfahrungen gerne mit. Jedoch fehlt oft die Zeit um alle Schüler ausreichend zu Wort kommen zu lassen und auf die spezifischen Bedürfnisse einzugehen. Zusätzlich nimmt die Interaktivität Zeit in Anspruch, sodass nicht immer alle wichtigen Punkte behandelt werden können. Deshalb wäre es sinnvoll die Schulungsdauer zu erhöhen. Denkbar wäre, dass sich die Schulung auf 2 Sitzungen verteilen würde. Bei der zweiten Sitzung könnten die Trainer überprüfen an was sich die Schüler noch erinnern und hätten ausreichend Zeit auf verschiedene Themen spezifischer einzugehen. Zudem könnten in der zusätzlichen Zeit praktische Übungen stattfinden. Auch die Lehrkräfte würden eine Verlängerung der Schulung und einen weiteren praktischen Teil befürworten. Zusätzlich wäre es wichtig, dass die Lehrkräfte selbst verstärkt medienpädagogisch tätig werden, indem sie Medien in den Unterricht mit einbinden und eigenständig die BEE SECURE Schulungen vor- bzw. nachbereiten oder ein ganzheitliches Konzept für ihr Schuljahr planen.

Bei dem neuen Begriff „Internet of things“ handelt es sich um Alltagsgegenstände, die, wenn sie mit dem Internet verbunden sind, miteinander bzw. mit einem anderen Gegenstand oder Gerät kommunizieren können. Dieses betrifft auch Kinderspielzeug wie bspw. intelligente Puppen, interaktive Tablets, übers Internet steuerbare Drohnen, sowie Kuscheltiere, die den Schlaf des Kindes überwachen. Auch wenn diese neuen Technologien Kinder geistig fördern und die technischen Fähigkeiten wecken können, so verbergen sie aber auch Risiken aus sowohl technischer als auch rechtlicher Natur in Bezug auf den Datenschutz. Daher wird die Sensibilisierung gerade in diesem Bereich zukünftig noch wichtiger.

Die Plattform „bee.lu“ wurde seit 2013 ausgebaut und soll auch in Zukunft erweitert werden. BEE SECURE ist es ein Anliegen schon den Kindern **ab 4 Jahren die Grundregeln** der sicheren Computernutzung altersgerecht zu vermitteln, denn Kinder finden immer früher den Weg ins Internet. Mittlerweilen sind 3 Geschichten von Bibi erschienen.

Daneben begrüßt BEE SECURE die Vielzahl an Veranstaltungen, die dazu beitragen die Sicherheitsbotschaften positiv zu vermitteln. So finden bspw. mehrmals jährlich die „Cryptoparty4kids“ oder auch die „Digirallye“ statt, die den Kindern einen näheren Einblick in die Technik der digitalen Welt bieten und somit die Möglichkeit eröffnen, Sicherheitsaspekte eher zu verstehen.

In Zukunft möchte BEE SECURE verstärkt Peer-to-Peer Trainings in den Schulen anbieten. Dabei werden ältere Schulklassen von BEE SECURE sensibilisiert um ihr Know-how anschließend an die Jüngeren weiterzugeben. Daneben wird auf Basis des Sicherheitskonzeptes der Jugendhäuser („secureMJ“), ein **Sicherheitskonzept für die Maison Relais** unter dem Namen „secureMR“ ausgearbeitet. Neben der Sicherung der technischen Infrastruktur sollen Erzieher und Kinder gemeinsam die Regeln für eine sichere Internetbenutzung erlernen. Ebenso hat die Universität Luxemburg ein Interesse geäußert, Medienerziehung in die **Ausbildung der Grundschullehrer** zu integrieren.

Nach zwei eher technischen Kampagnen widmet sich BEE SECURE im aktuellen Schuljahr 2016/2017 einem verhaltensorientierten Thema nämlich „SHARE RESPECT – Stop Online Hate Speech“. Unter Hate Speech versteht man, wenn Kommentare Hass oder Intoleranz ankurbeln gegen eine bestimmte Gruppe von Menschen z.B. aufgrund ihrer Religion, Nationalität, sexuellen Orientierung, ihres Geschlechts u.ä. Diese Worte können verletzen auch wenn sie nur getippt sind. Deshalb soll der respektvolle Umgang miteinander gefördert werden. Die aktuelle Kampagne bietet zum einen Handlungsstrategien, wie man auf Hate Speech in sozialen Medien reagieren kann, und zum anderen Präventionsstrategien, die darauf abzielen, dass sich eine durch Respekt gekennzeichnete Kommunikationskultur in den sozialen Medien entwickelt.