Sichereres Internet in den Jugendhäusern

Pädagogische Handreichung zum Sicherheitskonzept für Jugendhäuser

Stand August 2013

Index

Table of Contents

1 INDEX 2

2 EINLEITUNG 3

3 HANDLUNGSBEDARF 4

3.1 WARUM EINE CHARTA? 4

4 RÜCKBLICK 6

4.1 SCHULUNGEN ZUR IT-SICHERHEIT 6
4.2 SPEZIALFALL JUGENDHAUS 6
4.3 BESTANDSAUFNAHME 2007/08 7
4.4 MAßNAHMEN 2008 8
4.5 EVALUIERUNG DER UMSETZUNG 2012 9
4.6 AKTIONSPLAN SECURE MJ 2013 9

5 DAS SICHERHEITSKONZEPT IN DER PRAXIS 10

5.1 DIE CHARTA „SECURE MJ“ 10
5.1.1 LEITFADEN FÜR DEN ZUSTÄNDIGEN DER INFORMATIK UND COMPUTER IM JUGENDHAUS 10
5.1.2 LEITFADEN FÜR DAS BETREUUNGSPERSONAL IM JUGENDHAUS 19
5.1.3 BEE SMART VERHALTENSREGELN FÜR DAS JUGENDHAUS 26
5.2 PRAKTISCHE ANIMATIONEN 28
5.2.1 DISKUSSIONSERÖFFNUNG 29
5.2.2 AKTIVITÄTEN ZUM THEMA SELBSTDARSTELLUNG IM NETZ – PRIVATSPHÄRE 29
5.2.3 AKTIVITÄTEN ZUM THEMA BILDER IM INTERNET (RECHT AM EIGENEN BILD – COPYRIGHT) 30
5.2.4 AKTIVITÄTEN ZUM THEMA INFORMATIONEN IM INTERNET 31
5.2.5 AKTIVITÄT ZUM THEMA CYBERMOBBING 32
5.3 WEITERBILDUNG 33

1 Einleitung

Das vorliegende Dokument dient dazu, das Sicherheitskonzept, das für die Jugendhäuser in Luxemburg ausgearbeitet wurde, zu erklären und ergänzende Hilfestellungen, unter anderem durch eine Auswahl an Animationsmöglichkeiten, aufzulisten.

Die Publikation ist bewusst in einer vorläufigen Version herausgebracht. Weitere Erklärungen oder Ergänzungen werden auf Basis der Nutzer-Feedbacks hinzukommen.

Feedback kann gemailt werden an: snj@bee-secure.lu

2 Handlungsbedarf

2.1 Warum eine Charta?

Computer und Internet sind längst zu unverzichtbaren Hilfsmitteln geworden – auch in Jugendhäusern. Einerseits sind sie für die Erzieher ein wichtiges Arbeitsutensil: Sie helfen beim Verwalten von Daten, Organisieren von Veranstaltungen, beim Recherchieren und Archivieren. Andererseits sind sie, genau wie ein Tischfußball oder Flipper-Automat, ein Teil der Infrastruktur, der den jugendlichen Besuchern frei zur Verfügung steht.

Vom Gesetz vorgeschrieben ist der Internetzugang im Jugendhaus durch einen Eintrag im Memorial: „Pour un service d'information, les conditions supplémentaires suivantes à l'article 7 sont à respecter: 1. Disposer de locaux et d'équipements permettant l'accueil de jeunes, l'accès Internet étant obligatoire.[…]"[1] Über das Internet kann aber sowohl der Struktur des Jugendhauses als auch den Besuchern des Jugendhauses Schaden zugefügt werden. Mehrere Zwischenfälle aus den vergangenen Jahren haben bestätigt, dass Luxemburg sich diesen Herausforderungen nicht entziehen kann. Für den Bereich der Jugendhäuser haben sich gleich mehrere Akteure zusammengetan und ein für Luxemburg exemplarisches Pionierprojekt ausgearbeitet.

Von einer naiven Implementierung des Internetzugangs im Jugendhaus wird ausgegangen, wenn Jugendliche über das „Spielzeug Computer" Zugriff auf die professionellen Daten und Arbeitsvorgänge der Erzieher erhalten können. Dabei gilt die Devise: „Kleine Hindernisse sind keine Hindernisse". Denn leider zeigt die Erfahrung, dass Jugendliche nur selten über ihre Rechte und Pflichten im Internet aufgeklärt sind. Viele verfügen neben einem noch schwach ausgeprägten Respekt von Datenschutz und Privatsphäre auch über einige „Hacker"-Kompetenzen, was die Dringlichkeit einer obligatorischen Sicherheitscharta noch verstärkt.

In den Internetstuben der Jugendhäuser haben Jugendliche, die vielleicht zu Hause keinen Zugriff auf einen Computer haben, die Möglichkeit, Schulaufgaben am Rechner zu erledigen, sich in sozialen Netzwerken und Chats mit Freunden auszutauschen, oder anderen privaten Fragen und Interessen nachzugehen.

Die Betreiber der Jugendhäuser sind dazu verpflichtet, auf eine gewissenhafte und korrekte Benutzung dieser Internetstuben zu achten. Wer über Computer verfügt, muss sich auch einer enormen Vielfalt an sich ständig weiterentwickelnden Gefahren stellen. Es liegt in der Verantwortung des Jugendhauses, diese Gefahren zu vermeiden. Das Jugendhaus haftet nicht nur für Schäden oder Zwischenfälle, die von seinen Angestellten ausgehen, sondern auch für jene, die von Besuchern (den Jugendlichen) verursacht werden – egal ob wissentlich oder nicht. Schlimmstenfalls muss sogar mit einer Anklage der Eltern der betroffenen Jugendlichen gerechnet werden. Schließlich haben sie ihr Kind in die Obhut und damit auch in die Verantwortung der Erzieher im Jugendhaus gegeben. Dies gilt jedoch nur, wenn nachgewiesen werden kann, dass das Jugendhaus seiner Verpflichtung zur Informationssicherheit nicht nachgekommen ist. Haben Minderjährige trotz vorbildlich

[1] Memorial A n°9 vom 11. Februar 1999, Artikel 9

sicherer Infrastruktur die Regeln bewusst gebrochen, gilt nach wie vor: Eltern haften für ihre Kinder.[2]

Das Gesetz vom 2. August 2002 bezüglich persönlicher Daten[3] zwingt jeden Organismus, Sicherheitsmaßnahmen zum Datenschutz umzusetzen. Das Jugendhaus ist also rechtlich verantwortlich und muss im Ernstfall für entstandene Schäden haften.

Um die Risiken einzudämmen, denen Jugendliche beim Benutzen der neuen Technologien ausgesetzt sind, ist es wichtig, im Bereich der Prävention zu agieren. Dies geschieht durch Ausbildung, Sensibilisierung, jedoch auch durch die Einführung eines Leitfadens, beziehungsweise Regeln, die den sicheren und akzeptablen Umgang mit Internet und Mobiltelefon festlegen.

Im Rahmen seiner Mission behandelt das Jugendhaus sensible Informationen, die es zu schützen gilt. Um die Sicherheit dieser Daten zu gewährleisten, hat das Ministerium für Familie und Integration beschlossen, diese Sicherheitscharta ausarbeiten zu lassen und umzusetzen.

[2] Code Civil, Artikel 1384: « Le père et la mère, en tant qu'ils exercent le droit de garde, sont solidairement responsables du dommage causé par leurs enfants mineurs habitant avec eux. »
[3] Memorial A n°91 vom 13. August 2002: Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel

3 Rückblick

3.1 Schulungen zur IT-Sicherheit

Die ersten Präsentationen und Sensibilisierungskampagnen zum Thema Informations- und Computersicherheit gehen in Luxemburg auf das Jahr 2005 zurück, als das Ministerium für Wirtschafts- und Außenhandel (vertreten durch CASES[4]) und das Bildungsministerium eine Sensibilisierungsreihe in den Schulen ins Leben rief, um den sich häufenden Anfragen diverser Schulen nachzugehen. 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 und die Finanzierung der Schulungen verstetigt.
Nachdem die Durchführung 5 Jahre lang in den Händen von CASES lag, entstand mit der Gründung der interministeriellen Initiative BEE SECURE 2010 der perfekte Partner. Dem SNJ als Koordinator der Initiative obliegt seitdem auch die Verwaltung der Schulungen im Sekundarunterricht. Seither werden auch regelmäßig Sensibilisierungsaktionen in Jugendhäusern angeboten. Die erste fand 2009 in Hesperange statt.

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 Inhalte von BEE SECURE auf pädagogische Art und Weise an ihr Publikum weiterzugeben. Über ein Schuljahr verteilt werden alle Septima-Klassen des Landes abgedeckt. Andere Klassen sowie Grundschulen werden auf Anfrage auch besucht. Daneben werden spezielle Themenabende für Eltern, Senioren, Jugendhäuser und weitere Institutionen kostenfrei angeboten. Insgesamt werden derzeit pro Jahr über 550 Schulungen abgehalten.

3.2 Spezialfall Jugendhaus

Das Bedürfnis, speziell Jugendhäuser im Umgang mit den neuen Medien und Technologien zu sensibilisieren, wurde in den Jahren 2006 und 2007 deutlich, als zwei Vorfälle ein schlechtes Licht auf die Einrichtungen warfen:

- Innerhalb der Cyberstube, also dem Bereich, der den Jugendlichen zum Surfen im Internet zur Verfügung gestellt wird, hat ein Jugendlicher sich illegal Zugriff auf den Computer eines Erziehers und alle darauf befindlichen (teils geheimen und sehr sensiblen) Dateien verschafft. Das Hacking ist nicht zufällig passiert. Es war ein gezielter und erfolgreicher Angriff auf Informationen, die nicht zur Veröffentlichung bestimmt waren. Das informatische System war unzureichend geschützt.
- Von einem anderen Vorfall in einem anderen Jugendhaus erfuhren die Erzieher erst, als die Polizei vor der Tür stand und nach einer genauen Auskunft fragte: „Wer hat am Tag X um Y Uhr den Computer mit der IP-Adresse Z in diesem Haus benutzt?“ Der Grund für die Aufregung: Eben dieser gesuchte Jugendliche hatte zu gefragtem Zeitpunkt den Computer zum Hacking missbraucht. Da er bei seinen kriminellen Ausflügen ins Netz illegale Aktivitäten unternahm, leitete der Internet Service

[4] Cyberworld Awareness & Security Enhancement Services, www.cases.lu

Provider die IP-Adresse an die Polizei weiter. Die wiederum suchte den Schuldigen – und auch den Verantwortlichen – im Jugendhaus.

Diese Zwischenfälle sowie ähnliche Vorkommnisse in weiteren Jugendhäusern des Landes, veranlassten die Erzieher selbst zum Nachdenken. Sind sie IT-technisch fit genug, um kriminelle Aktivitäten in Zukunft zu unterbinden? Inwiefern können sie für Vergehen ihrer Schützlinge zur Rechenschaft gezogen werden? Welche Rolle spielen sie als Vermittler eines bewussten und sicheren Umgangs mit dem Internet? Diese Fragen stellten u.a. die Erzieher aus dem Jugendhaus Petange. Den öffentlichen Akteuren (MiFa, SNJ) war ihrerseits bewusst, dass diesen Fragen konkrete Handlungslösungen entgegengebracht werden sollten.

3.3 Bestandsaufnahme 2007/08

Die Zwischenfälle und die aufgeworfenen Fragen seitens der Erzieher haben einen auch jetzt noch andauernden Handlungsprozess ausgelöst. Den Anfang bildete dabei eine Bestandsaufnahme, die das Familienministerium und der „Service National de la Jeunesse“ 2007 bei CASES in Auftrag gaben.

Die Erkenntnis: Computer und Internet waren in den untersuchten Jugendhäusern unzureichend geschützt.

- Technische Maßnahmen wie Antivirenprogramm und Firewall waren nur dürftig installiert und oft nicht auf dem neusten Stand gehalten.

- Internetfilter gab es keine. Alle Computer, sowohl die der jugendlichen Besucher, als auch die der Erzieher, waren an ein und dasselbe Netz gekoppelt. Dies führte dazu, dass alle denselben Zugriff auf dasselbe uneingeschränkte Internet hatten. Im Klartext: Ein 10-jähriges Kind konnte ebenso problematische Inhalte (Pornografie, Rassismus,…) anschauen, wie ein 19-jähriger junger Erwachsener. Schaut sich jedoch ein Kind unter 16 Jahren einen solchen Inhalt an, ist dies rechtswidrig[5] und das Jugendhaus in der Verantwortung! Ein weiterer Haken der barrierefreien Netze: Jugendliche konnten von ihren Computern schnell Zugriff auf die (zum Teil streng vertraulichen) Daten der Erzieher erlangen. Schlecht ausgewählte, simple Passwörter seitens der Erzieher erleichterten den jungen Hackern zusätzlich das Spiel.

- Spätestens hier wurde klar: Jugendhäuser brauchen logistisch voneinander getrennte Netze. Der Raum, in dem Jugendliche surfen, muss ein anderer sein, als der, in dem sich ihre Erzieher bewegen.

- Oft wurde den Jugendlichen freie Hand überlassen, was die Konfiguration der Computer betraf. Programme (auch schädliche oder so genannte „Hackerprogramme“) konnten leicht aus dem Internet heruntergeladen und auf dem Computer installiert werden. Genauso Filesharing-Software.

- Musik und Filme wurden häufig in den „Internetstuben“ heruntergeladen – ungeachtet geltender Bild- und Autorenrechte. Dass dies eine illegale Aktivität ist,

[5] Gesetzestext

störte die jungen Musikfreunde ab und zu genau so wenig wie die Erzieher, die mit derart heruntergeladener Musik und Filmen das Jugendhaus animierten.

- Zwar gab es in den meisten Jugendhäusern einige Regeln bezüglich des Internet- und Computergebrauchs, doch stützten sich diese meist auf den Faktor der Zeit: Jugendliche sollten nicht zu viel Zeit am Computer verbringen, da sie sonst den sozialen Austausch mit anderen vernachlässigten. Was vollkommen fehlte, waren sicherheitsrelevante Regeln, wie zum Beispiel das Benutzen von starken Passwörtern, das Untersagen illegaler Downloads, das Nicht-Aufrufen illegaler Seiten, der bedachte Umgang mit E-Mail, Messenger, sozialen Netzwerken usw. oder der gegenseitige Respekt im Internet.

Konfrontiert mit den Sicherheitsmängeln fühlten sich viele Erzieher und Betreiber von Jugendhäusern hilflos und zu sehr in die Verantwortung gezogen. Tatsache ist jedoch: Als Betreuungseinrichtung für Jugendliche über einen gewissen Zeitraum sind die Jugendhäuser per se in der Verantwortung. Auch rechtlich müssen sie für Schäden aufkommen und sind haftbar, wenn ihre Schützlinge innerhalb des Jugendhauses illegal handeln.

Eine Regulierung des Computer- und Internetgebrauchs ist keine Kontrolle und keine Machtentnahme. Sie ist ein notwendiger und legitimer Schritt zur Medienerziehung und möglichst sicherem – und dadurch auch effektiverem- Gebrauch der neuen Medien.

3.4 Maßnahmen 2008

Auf Basis der vorher gewonnenen Stärken und Schwächen im Umgang mit den neuen Technologien, haben das Familienministerium, der SNJ und CASES 2008 einen konkreten Aktionskatalog umgesetzt:

- **Regelmäßige Weiterbildungen** zum Thema neue Medien wurden in den Weiterbildungskatalog aufgenommen. Sicherheit ist kein Zustand, sondern ein kontinuierlicher Prozess. Den Betreibern und Erziehern der Jugendhäuser wurde deshalb die Wichtigkeit vermittelt, an Sensibilisierungs- und Schulungsangeboten im Bereich der Informationssicherheit teilzunehmen, um ihre Kenntnisse regelmäßig auf den neusten Stand zu bringen.

- Auch nicht-permanente Mitarbeiter und die jugendlichen Besucher selbst sollten an **Sensibilisierungsaktionen** teilnehmen, um sich ihrer Rechten und Pflichten, ihrer Verantwortung und den Konsequenzen im Fall von Nicht-Respektieren der Regeln bewusst zu werden. Die BEE SECURE – Sessions wurden alljährlich angeboten.

- Den Jugendhäusern wurde eine **umfassende Sicherheitspolitik** mit den entsprechenden zu ergreifenden Maßnahmen vorbereitet. Diese Sicherheitspolitik erklärte, wie man Risiken mindert, ohne den Aktionsraum einzuschränken. Sie definierte die technischen Maßnahmen, die im Sinne der Informationssicherheit durchgeführt werden sollten, legte Perimeter für die physische Sicherheit fest, definierte Prozeduren für die Verwaltung sensibler Informationen, den Umgang mit E-Mails, WiFi, Passwörtern usw. Gesetzlich ist jeder dazu verpflichtet, Autorenrechte und geistiges Eigentum zu schützen. Auch persönliche Daten müssen geschützt werden.

- In Zusammenarbeit mit der EGMJ wurde eine kostengünstige **technische Schutzvorrichtung** ausgearbeitet und in allen Jugendhäusern installiert (Projet „Secure MJ“). Damit konnten die Computer von Erziehern und Jugendlichen getrennt sowie der Zugang der Jugendlichen im rechtlichen Rahmen eingeengt werden.

3.5 Evaluierung der Umsetzung 2012

2012 wurden die durchgeführten Maßnahmen auf ihre Umsetzung und ihre Zweckmäßigkeit überprüft.

- Die Weiterbildungen fanden alljährlich statt, aber durch den relativ großen Personalwechsel in den Jugendhäusern sind nicht alle Jugendhäuser gleich gut informiert. Neu eingestellte Erzieher wussten oft nichts zum Projekt.

- Die technische Schutzmaßnahme (Secure MJ) wurde nicht immer permanent eingesetzt. So wurde gelegentlich die Firewall umgangen oder aber ein WiFi vorgeschaltet, so dass die Jugendlichen auf den PCs ein jugendgerechtes Surfen kannten, die WiFi-Nutzer aber einen ungeschützten Zugang zum Internet hatten.

- Eine regelrechte Sicherheitspolitik wurde kaum umgesetzt. Das erarbeitete Musterdokument bedarf zwar einer geringen Anpassung an die jeweiligen Jugendhäuser, aber wohl alleine durch den Seitenumfang hat es viele abgeschreckt.

3.6 Aktionsplan Secure MJ 2013

Das Familienministerium hat Internet in den Jugendhäusern zur Verpflichtung gemacht. Damit ist jeder Betreiber („Gestionnaire“) verantwortlich dafür, dass in seinem Jugendhaus ein Internetanschluss für Mitarbeiter und Besucher gegeben ist. Der Betreiber übernimmt auch die Verantwortung dafür, dass die Sicherheitsbestimmungen erfüllt werden. Die Charta Secure MJ hilft ihm dabei.

Informationssicherheit darf in Jugendhäusern keine Option sein, sondern eine Voraussetzung zur Nutzung der neuen Medien. Medienerziehung wird damit zu einem Pflichtfach für alle, die Internet, Smartphone, Tablet, Computer und Co benutzen – egal ob Erzieher oder Jugendlicher. Dieser Überzeugung liegt die 2013 an allen Jugendhäusern eingeführte Charta „Secure MJ“ zugrunde.

Im nächsten Kapitel werden die einzelnen Komponenten des Aktionsplans im Detail erklärt.

4 Das Sicherheitskonzept in der Praxis

Es gibt insgesamt 4 Dokumente, die ausgearbeitet wurden, und die für alle Jugendhäuser verbindlich sind.

Das erste Dokument ist ein Formular des Familienministerium, in dem der Betreiber des Jugendhauses belegt, wie er die Sicherheit im Jugendhaus umsetzt und wer für welchen Sicherheitsaspekt verantwortlich ist. Dieses Dokument wird Bestandteil der Betriebserlaubnis (Agrément) und verweist auf die drei Chartas, die in jedem Jugendhaus angewandt werden müssen:

- **Die erste Charta richtet sich an den operationellen Zuständigen (OZ), den informatischen Kopf des Hauses. Er wird im Vorfeld vom Betreiber des Jugendhauses designiert.**
- **Die zweite Charta richtet sich an das feste Personal des Jugendhauses, also die Gesamtheit der Erzieher.**
- **Bei der dritten Charta handelt es sich um eine redaktionell schlicht gehaltene Auflistung von Basis-Sicherheitsregeln für die Jugendlichen. Sie sind als Poster jugendgerecht verpackt und leicht verständlich.**

Die Chartas sind von ihren jeweiligen Zielgruppen gründlich durchzulesen, denn sie bilden das Gerüst für Informationssicherheit im Jugendhaus. Jeder Betroffene verpflichtet sich, die beschriebenen Regeln zu respektieren, indem er „seine“ Charta unterzeichnet. Bei den Jugendlichen kann es reichen, dass die Charte gut sichtbar in der Nähe der Computer angebracht ist.

Folgende sicherheitsrelevanten Aspekte müssen von einem Jugendhaus umgesetzt werden:

- **Trennung der Netze (via Firewall)**
- **Installation und regelmäßiges Updaten von Antivirenprogrammen**
- **Filterung des Internetzugangs von Jugendlichen**
- **Backup der Daten**
- **Sensibilisierung der Jugendlichen**
- **Weiterbildung des Personals des Jugendhauses (Erzieher)**

4.1 Die Charta „Secure MJ“

4.1.1 Leitfaden für den Zuständigen der Informatik und Computer im Jugendhaus

1.1. Was sind die Aufgaben des operativen Zuständigen?

Der operationelle Zuständige (OZ) sorgt dafür, dass die Erzieher-Charta mit Empfangsbestätigung an das bereits bestehende Personal sowie an alle neuen Mitarbeiter

verteilt wird. Er muss eingreifen, wenn er feststellt, dass die Charta nicht respektiert wird. Darüber hinaus muss er kontrollieren, ob alle technischen oder organisatorischen Änderungen im Jugendhaus mit der Charta „Secure MJ“ vereinbar sind. Besteht eine Situation, die nicht der Charta entspricht, und die nicht lokal gelöst werden kann, muss der OZ den Verwalter des Jugendhauses hierüber in Kenntnis setzen.

1.2. Information beherrschen

In Jugendhäusern gibt es 2 Arten sensibler Informationen:

1) Operationelle Daten:
   Alle Daten und Dokumente, die zum Funktionieren des Jugendhauses benötigt werden. Diese Dokumente können durchaus von vertraulicher Natur sein und sich zum Beispiel auf Buchhaltung, Gehälter, Rechnungen, wichtige Mitteilungen oder Verträge beziehen.
2) Persönliche Daten:
   Alle Daten und Dokumente, die Informationen über namentlich erwähnte Personen (interne oder externe) enthalten, wie zum Beispiel persönliche Notizen, Anwesenheitslisten, Internetprotokolle usw. Informationen dieser Art sind vertraulich.

Es obliegt der Verantwortung des OZ, zu ermitteln, welche spezifischen Daten gespeichert werden müssen, zu welcher Kategorie (operationell oder persönlich) sie gehören, und wie sie aufbewahrt werden müssen. Er muss sich die Frage stellen, ob es nur elektronische Kopien der Daten gibt, oder ob sie zum Beispiel auch in Papierform archiviert werden. Egal wie er sich entscheidet, muss er dafür sorgen, dass die Daten sicher und den Gesetzen zum Datenschutz und Schutz der Privatsphäre entsprechend verwahrt werden und nicht in die falschen Hände gelangen können.

Informationen, wie etwa zum familiären Hintergrund oder zu charakterlichen Auffälligkeiten eines jugendlichen Besuchers, mögen für den Erzieher eine wichtige Information sein, die notwendig ist, damit er in seiner Arbeit auf die spezifischen Bedürfnisse des Jugendlichen eingehen kann. Solche Daten dürfen jedoch auf keinen Fall nach draußen oder an den Jugendlichen selbst dringen. Dies hätte katastrophale Auswirkungen auf das Vertrauensverhältnis zwischen Jugendlichem und Erzieher und schlimmstenfalls auch gerichtliche Konsequenzen, da geltende Gesetze missachtet wurden.

1.2.1. Den Zugang zur Information kontrollieren

Der OZ bestimmt, welche Information von welchen Personen einsehbar ist, wie und ob sie geteilt werden darf, und wie mit ihr umgegangen wird. Grundsätzlich gilt: Zugriff auf die Information hat nur, wer ihn für professionelle Zwecke benötigt. Der **Verteilungsradius einer sensiblen Information muss so klein wie möglich gehalten** werden, um Missbrauch vorzubeugen. Ein Erzieher zum Beispiel benötigt keinen Zugang zur Buchhaltung des Jugendhauses, und ein Praktikant braucht keinen Aufschluss über den Gesundheitszustand eines jugendlichen Besuchers. Nur Informationen, die für die tägliche Arbeit benötigt werden, werden den entsprechenden Teammitgliedern mitgeteilt. Es wäre ein Fehler, systematisch allen Mitarbeitern Zugriff auf alle Daten und Dokumente zu gewähren. Je mehr Personen eine sensible Information einsehen können, umso größer ist die Gefahr, dass sie (bewusst oder ungewollt) nach außen dringt oder missbraucht wird.

Gleiches gilt in Bezug auf Rechte bei der Computernutzung. Hier muss vom **Prinzip des geringsten Privilegs** ausgegangen werden: Einer Person sollen keine Rechte zugestanden werden, die sie nicht unbedingt benötigt. Wenn alle Programme, die eine Person zur Arbeit am Computer benötigt, bereits auf dem Gerät installiert sind, ist es überflüssig, ihr das Recht zu gewähren, noch zusätzliche Programme darauf zu installieren. Dies ist wichtig, um zu verhindern, dass Schadsoftware auf den Computer gelangt (etwa durch Downloads aus dem Internet oder unsaubere Raubkopien), dass ein Computer für unlautere Zwecke missbraucht wird, oder dass der OZ den Überblick über die Computernutzung verliert.

Dass der Zugang zur Information stark eingeschränkt ist, bedeutet nicht, dass den Mitarbeitern und Teamkollegen misstraut wird. Es ist lediglich ein notwendiger Schutzprozess, um im Fall einer Fehlerhandlung den Schaden so gering wie möglich zu halten. Wenn dann zum Beispiel ein Benutzername und Passwort geknackt werden, hat der Eindringling nur Zugriff auf eine beschränkte Auswahl an Informationen. Damit ist auch das Ausmaß der Folgen seines illegalen Eindringens beschränkt.

1.2.1.1.

Firewall im Secure-MJ-Gehäuse

Eine Firewall ist ein Sicherungssystem, das ein Netzwerk vor unerwünschten Zugriffen schützt. Sie basiert auf einem Programm, das den durch die Firewall laufenden Datenverkehr überwacht. Dies passiert nach im Vorfeld festgelegten Regeln. Im Fall der Jugendhäuser blockiert die Firewall jegliche Internetprotokolle, abgesehen von E-Mail und Web sowie verschiedenen Protokollen, die für technische Vorgänge benötigt werden, wie zum Beispiel zum Updaten des Antivirenprogramms oder vom Secure-MJ-Gehäuse stammen.

Im Secure-MJ-Gehäuse ist die Firewall mit einem Antivirenprogramm kombiniert, der permanent den Internetverlauf auf Schadprogramme scannt. (Ein weiteres Virenprogramm muss auf den einzelnen Computern im Jugendhaus installiert sein.)

Einteilung des Netzes in drei Zonen

Grundvoraussetzung für eine gelungene Kontrolle des Zugriffs auf Informationen ist die Einteilung des internen Netzes in 3 Zonen (Vertrauensbereiche), die im Prinzip keinen Austausch untereinander erlauben. Jedoch können die Firewall-Regeln in spezifischen Fällen angepasst werden, sodass dennoch ein Austausch zwischen 2 Netzen stattfindet. Die 3 Zonen ermöglichen allen Beteiligten eine an ihre Bedürfnisse und Befähigungen angepasste Benutzung des Internets und der informatischen Systeme im Jugendhaus. Sie sind, entsprechend den Zuständigkeiten ihrer Benutzer, an verschiedene Freiheiten gebunden. Alle Zonen sind an den Internetverteilerkasten „Secure MJ“ gekoppelt, der mit Firewall und Antivirenprogramm ausgestattet ist.

- Die erste Zone heißt „Jugend“ und umschließt das Internet im Cyberbereich des Jugendhauses. Diese Zone wird von den jugendlichen Benutzern beansprucht und darf keinerlei sensible Informationen oder Daten enthalten. Sie dient zum Arbeiten am Computer und Surfen im Internet unter Vorbehalt problematischer Inhalte. Das

Internet, auf das die Jugendlichen Zugriff haben, ist gefiltert. So wird verhindert, dass Minderjährige in Kontakt mit gefährdenden oder illegalen Inhalten kommen. Downloads werden blockiert und kontrolliert, bevor sie nach Einschätzung des OZ freigegeben werden, oder auch nicht. Die Einschränkungen in dieser Zone sind ausreichend, um den Jugendschutz zu gewährleisten und dennoch nicht so restriktiv, dass Recherchen oder Freizeitaktivitäten im Internet darunter leiden würden. Hat ein Benutzer das Gefühl, von der Zone zu stark eingeschränkt zu sein, kann er sich an das Personal und bestenfalls den OZ wenden, mit der Bitte, vorübergehend auf ein weniger eingeschränktes Netz (Mittelzone) zugreifen zu dürfen. Dem OZ obliegt die Verantwortung für alles, was in dieser Ausnahmesituation über den Rechner passiert.

- Die zweite Zone heißt „Betreuungspersonal“ und richtet sich auch an selbiges. Sie darf nur von hauptamtlichen Mitarbeitern benutzt werden (nicht von Zeitarbeitern oder Praktikanten), da sie den Zugriff auf sensible Informationen gewährt. Es ist unbedingt notwendig, dass sich das Betreuungspersonal über ein starkes Passwort in das Netz loggt. Login-Daten dürfen unter keinen Umständen an die Jugendlichen oder an sonstige Personen außerhalb des berechtigten Kreises gelangen, um Missbrauch und Verletzung des Datenschutzes zu verhindern.

- Die dritte Zone ist die „Mittelzone“. Sie kann am besten an individuelle Bedürfnisse angepasst werden. Somit eignet sie sich als Zone für nicht-permanente Mitarbeiter oder auch für Jugendliche, denen im Rahmen eines Projektes (z.B. Recherchen als Jugend-Reporter oder während eines Medienprojekts) mehr Freiheiten im informatischen System zugestanden werden. Über diese Zone gibt es keinen Zugriff auf sensible Daten. Sie lässt sich entsprechend der aktuellen Bedürfnisse individuell konfigurieren. Darüber hinaus kann über die Mittelzone das kabellose Internet (WiFi) laufen, auf das die Jugendlichen und/oder das Begleitpersonal im Jugendhaus zugreifen können. Natürlich obliegt auch dieses kabellose Internet dem Filterprogramm des Verteilerkastens „Secure MJ“. Wenn ein Jugendhaus gleichzeitig WiFi und eine Internetzone für nicht-permanentes Personal einrichten möchte, muss ein Interface zugefügt werden.

Um zu vermeiden, dass es zu unbefugtem Zugriff durch nicht berechtigte Benutzer kommt, sind die 3 Zonen streng voneinander getrennt. Jeder Benutzer muss sich anhand eines Benutzernamens und eines Passworts identifizieren. So kann der OZ kontrollieren und nachweisen, wer sich zu welchem Zeitpunkt in welcher Zone aufgehalten hat.

Die Trennung der Netze ist wesentlich, um eine Kontrolle des Internets und Absicherung der informatischen Vorgänge im Jugendhaus a priori zu gewährleisten. Sie ermöglicht mit einfachen Mitteln die Vergabe von individuell abgestimmten Rechten. So wird der gesicherte Zugriff zum Internet, der Zugriff auf Information sowie der präventive Schutz vor Schädlingen stark vereinfacht. Nach diesem Prinzip funktionieren alle Jugendhäuser.

Internetfilter im Secure-MJ-Gehäuse

Im Gehäuse befindet sich ein Internetfilter, der einen kontrollierten und an die verschiedenen Zonen angepassten Datenaustausch ermöglicht. Die Standardeinstellung sieht dabei eine Negativliste („blacklist“) für folgende Themen vor: Proxy illegale Programme, Filesharing, Gewalt, Hacking, Gefahrengut (z.B. Anleitung zum Bauen von Bomben, Herstellen von Waffen, usw.) Pornografie ist zwar, sofern von Erwachsenen konsumiert, nicht illegal, darf aber für Minderjährige nicht frei zugänglich sein. Es wird dazu geraten, auch pornografische Inhalte auf die Negativliste zu setzen.

Der OZ hat die Möglichkeit, für jeden einzelnen Internetposten im Jugendhaus diese Blacklist zu bearbeiten, d.h. einzelne Themen freizuschalten. Natürlich geht mit diesem Recht auch eine enorme Verantwortung einher. Für Jugendliche ist das generelle Filtern des Internets ein wichtiger Aspekt für mehr Sicherheit. Es versteht sich also von selbst, dass der Filter auf Computern, die von Jugendlichen benutzt werden, nicht gelockert werden sollte. Der Erzieher hat die Möglichkeit, Positivlisten („white lists“) und Negativlisten selbst zu verwalten. Damit kann er zum Beispiel den Zugriff auf einen der folgenden Inhalte zulassen: Dating, Finanzen, Audio-Video, Spiele, Werbung, Blogs, Drogen oder Astrologie. Um mehr Sicherheit zu gewähren, muss der Zugriff auf Informationen im Internet kontrolliert werden.

Warum lohnt es sich, Kinder und Jugendliche vor problematischen Inhalten im Netz zu schützen?

Im Internet gibt es eine riesige Anzahl an Webseiten mit problematischen Inhalten. Dazu gehören Pornografie, politischer Extremismus, Gewaltdarstellung bzw. -verherrlichung und selbstgefährdende Inhalte wie zum Beispiel Drogen-, Selbstverletzungs-, Depressions- und Suizidforen oder die Verherrlichung von Essstörungen unter den Pseudonymen „Pro-ANA“ (Anorexie) und „Pro-MIA“ (Bulimie).

Besonders auf Kinder und Jugendliche üben solche Inhalte einen gefährlichen Reiz aus. Sie lassen sich generell leicht von Onlinegemeinschaften faszinieren, denn diese bieten die Möglichkeit, Gleichgesinnte kennenzulernen und sich mit ihnen rund um die Uhr auszutauschen. In der emotionalen Entwicklungsphase, in der sich Jugendliche befinden, entsteht schnell ein Zusammengehörigkeits-, ein „Wir“-Gefühl. Gefährlich wird es dann, wenn Jugendliche die anfangs „nur mal so aus Neugierde“ reingeklickt haben, sich plötzlich mit der virtuellen Community identifizieren und sich im realen Leben von ihr beeinflussen lassen.

Beim Anschauen von Gewalt- und Pornovideos hingegen erfahren viele einen emotionalen „Kick“. Zu wissen, dass die Inhalte problematisch sind, verstärkt ihre Wahrnehmung als ein „aufregendes Erlebnis“. Häufig handelt es sich dabei auch um Gemeinschaftserlebnisse, bei denen besonders extreme Inhalte zur Anerkennung genutzt werden.

Verzerrte Wahrnehmung von Körper- und Schönheitsidealen, von Sexualität und dem sozialen Miteinander in der Gesellschaft können dazu führen, dass Betroffene den Bezug zur Realität verlieren.

1.2.1.2.

Informationen auf Papier oder Wechseldatenträgern

Werden Informationen auf Wechseldatenträgern, z.B. auf USB-Sticks oder externen Harddiscs gespeichert, oder auf Papier gedruckt und archiviert, muss dafür gesorgt werden, dass der physische Zugriff darauf eingeschränkt wird. Im Klartext: Alle Datenträger, egal ob technisch oder aus Papier, müssen in Safes, abschließbaren Schränken oder abgesperrten Räumlichkeiten aufbewahrt werden. Zugang wird nur jenen Personen gewährt, die zum korrekten Ausführen ihrer Arbeit Einsicht in diese Daten haben müssen. Dabei ist es wichtig, Regeln für den Umgang mit Schlüsseln aufzustellen. Es muss definiert werden, wer vom Personal einen Schlüssel zum Aufbewahrungsort der Speichermedien erhält und wo dieser Schlüssel aufbewahrt werden muss. Es versteht sich von selbst, dass eine vorbildliche Archivierung von Daten sinnlos ist, wenn unbefugte Personen jederzeit den Schlüssel entwenden und die sensiblen Daten einsehen könnten.

Das gesamte Erzieher-Team des Jugendhauses muss darüber informiert sein, wie Daten archiviert werden und wie der Zugriff auf sie verwaltet wird.

1.2.2.

Datensicherung (Backups)

Die Sicherung von Daten ist von entscheidender Bedeutung für jedes informatische System. Denn ein Datenträger ist nur während einer bestimmten Zeit zuverlässig. Außerdem muss mit äußeren Einflüssen wie Schadsoftware oder menschlichen Fehlern (aus Versehen gelöscht) gerechnet werden. Damit sensible Daten dabei nicht auf dem Spiel stehen, muss eine Backup-Strategie umgesetzt werden. Dies bedeutet, dass eine Datensicherung in regelmäßigen Abständen (die Wichtigkeit der Daten entscheidet über die Frequenz) und nach einem vorher definierten System durchgeführt wird.

Tipps zur Wahl des Datenträgers:

- Wechseldatenträger (CD, DVD, USB-Stick): sehr preiswert aber von geringer Datenkapazität und nicht lange haltbar; aus diesem Grund wird heutzutage nicht mehr geraten, diese Datenträger für Sicherungen zu benutzen (außer vielleicht für sehr geringe Volumen).
- Magnetische Festplatten (externe Harddisks): kostengünstig, bieten die größten Datenkapazitäten und widerstehen recht gut der Degradierung und dem zeitlichen Verfall.
- Onlinedienste (Cloud): Preis, Verfügbarkeit und Lebensdauer hängen sehr vom Anbieter ab; werden aber dank der hohen Übertragungsrate, die mit Glasfaser selbst den kleinsten Unternehmen zur Verfügung steht, immer interessanter. Derzeit wird aber geraten, Cloud-Lösungen vor einer Zusage gut zu kontrollieren, vor allem dahingehend, wie seriös der Anbieter ist. Cloud Computing bietet sich gut für konstante Backups an.

Backups sollten regelmäßig gemacht werden. Je öfter, desto weniger Daten gehen im Ernstfall verloren. Falls Sie einmal in der Woche eine Datensicherung machen, werden Sie die Arbeit von höchstens einer Woche verlieren. Da der Speicherplatz begrenzt ist, empfiehlt sich eine Datensicherungsrotation. Es muss entschieden werden, welche Sicherungen Sie wieder mit neuen überschreiben können. Bei der wöchentlichen Datensicherung empfiehlt es sich, die sechs letzten Sicherungen aufzubewahren, um so über die Sicherung eines ganzen Monats verfügen zu können.

Es versteht sich von selbst, dass die Sicherungskopien der sensiblen Daten mit derselben Sorgfalt und denselben Vorsichtsmaßnahmen behandelt werden müssen, wie die Originaldaten. Im Idealfall werden die Sicherungskopien außerhalb des Jugendhauses aufbewahrt, um bei unvorhersehbaren Schadensfällen (z.B. bei Feuer oder Vandalismus) einen Totalverlust der Daten zu verhindern.

1.3. Physische Sicherheit des informatischen Materials

Das Router-Material des Secure-MJ-Kastens muss im dafür vorgesehenen Gehäuse aufbewahrt werden. Das Gehäuse ist verschlossen, und der Schlüssel muss so aufbewahrt werden, dass unbefugte Personen keinen Zugriff darauf haben. So kann Manipulation vorgebeugt werden.

Die Anordnung der einzelnen Computerposten im Raum darf nur dann verändert werden, wenn eine gefahrlose Verkabelung möglich ist. Dies bedeutet, dass Kabel so verlaufen müssen, dass keine Stolpergefahr besteht, und weder Kinder noch Personal Stromschläge durch mangelhafte Anschließung oder fehlende Sicherung riskieren.

1.4. Schutz vor Schadprogrammen

Unabhängig von dem bereits im Secure-MJ-Gehäuse installierten Antivirenscanner, muss jeder einzelne **Computer mit einem Antivirenprogramm** ausgestattet sein. Dieses scannt den lokalen Computer automatisch auf Schädlinge und schlägt Alarm, wenn zum Beispiel ein Virus in einer verdächtigen E-Mail oder auf einem externen USB-Stick entdeckt wird.

Die meisten Antivirenprogramme gibt es im kompletten Sicherheitspaket mit integrierter Firewall, Anti-Spyware, Phishing-Schutz und Webfilter. Man kann sie entweder kaufen oder gratis im Internet herunterladen. Nicht immer sind die gekauften Programme besser als die kostenlosen. Erstere bieten nur meist noch weitergreifende Funktionen an, während Gratisprogramme hin und wieder (ungefragt) auf die Vorteile der kommerziellen Variante hinweisen.

Egal ob gratis oder kostenpflichtig: Das Wichtigste ist eine **regelmäßige Aktualisierung** des Programms und der zugehörigen Datenbanken, um neue Schadprogramme zu erkennen. Denn alte Software-Versionen bieten eine einfache Angriffsfläche für Schadprogramme. Praktisch ist es, wenn man das Antivirenprogramm so einstellt, dass es verfügbare Updates automatisch installiert. Andernfalls muss eine dazu befugte Person dafür sorgen, dass das Programm manuell immer auf dem neusten Stand gehalten wird.

Als weiterer Schutz vor Schadprogrammen ist es wichtig, **regelmäßig Patches zu installieren**. Patches sind Updates oder „Flickprogramme“, die von Software-Herstellern entwickelt werden, um Schwachstellen in ihren Programmen auszubessern und Sicherheitslücken zu schließen. So kann man verhindern, dass Kriminelle die bestehenden Sicherheitslücken ausnutzen, um Schadprogramme einzuschleusen. Oft wird mit dem Patch die Software zusätzlich um neue Funktionen ergänzt. Man sollte sich regelmäßig über aktuelle Sicherheitslücken informieren und die neusten Patches installieren. Das Sprichwort „Never touch a running system“ trifft in der Sicherheit nicht zu.

1.5. Sicherheit der kabellosen Verbindungen – WiFi

Wenn im Jugendhaus kabelloses Internet angeboten wird, muss dieses über die dafür vorgesehene Mittelzone laufen. Nur so kann sichergestellt werden, dass das Internet auch in diesem Fall gefiltert wird, und Jugendliche keinen Zugriff auf problematische Inhalte haben.

1.6. Konform zur Gesetzgebung

1.6.1. Autorenrechte

Das Jugendhaus muss sicherstellen, dass alle benutzten Programme und Betriebssysteme auf legale Art und Weise erworben wurden. Bei Software, die Lizenzbestimmungen unterliegt, muss diese Lizenz im rechtmäßigen Besitz des Jugendhauses sein. Ansonsten darf die Software nicht benutzt werden.

Eine empfehlenswerte Adresse für legale Software ist z.B. http://www.socialware.be. Hier gibt es für relativ wenig Geld eine große Auswahl an Programmen.

Es soll dran erinnert werden, dass Software (ebenso wie Hardware) im Budget des Jugendhauses vorzusehen ist. Dies kann im Rahmen einer kompletten Neuanschaffung sein (Stichwort „premier équipement“), oder im Rahmen eines einzelnen Softwarekaufs.

1.6.2. Benutzer informieren

Das Dokument „Die 10 Internet-Gebote“ dient dazu, einem jugendlichen Publikum auf simple und einprägsame Art und Weise Basisregeln für einen sicheren Gebrauch der neuen Medien nahe zu bringen. Der OZ muss dafür sorgen, dass die Besucher des Jugendhauses dieses Dokument einsehen können. Dazu soll es an alle Internetbenutzer verteilt werden und / oder so im Raum aufgehängt werden, dass es für alle vom Computer aus gut sichtbar ist.

Darüber hinaus beinhaltet das Dokument einen weiteren sehr wichtigen Punkt: Die Jugendlichen werden **darüber in Kenntnis gesetzt, dass ihr Surfverhalten gespeichert** und ggf. kontrolliert werden kann. Da dies einen sensiblen Eingriff, zum Teil auch in die Privatsphäre der Jugendlichen darstellen kann, müssen diese darüber informiert werden. Kein Benutzer soll später behaupten können, nichts von der Kontrolle und dem Speichern seines Surfverhaltens gewusst zu haben. Der Hinweis darauf ist deshalb obligatorisch!

Es liegt in der Verantwortung der Erzieher, den Jugendlichen den Sinn und Zweck der „SMART-Verhaltensregeln“ zu erklären, und ihnen diesbezüglich Rede und Antwort zu stehen.

4.1.2 Leitfaden für das Betreuungspersonal im Jugendhaus

1.1. Einleitung

Dieser Leitfaden richtet sich an das betreuende Personal, also die Erzieher im Jugendhaus und muss jedem einzelnen von ihnen bekannt sein. Es liegt in der Verantwortung des operationellen Zuständigen (OZ), allen Erziehern diesen Leitfaden zu unterbreiten. Er enthält eine Zusammenfassung der anzuwendenden Regeln im Umgang mit Computer, Internet und der Secure-MJ-Box. Diese Regeln beschreiben das Mindestmaß an Sicherheitsvorkehrungen und müssen in jedem Jugendhaus appliziert werden.

1.2. „Die 10 Internet-Gebote“

Die erste Verantwortung der Erzieher in Bezug auf Internet und Computer besteht darin, die Jugendlichen auf das Dokument „Die 10 Internet-Gebote“ aufmerksam zu machen. Dieses Dokument erklärt auf eine jugendfreundliche Art und Weise, warum man sich im Internet an bestimmte Regeln halten muss. Erzieher sollten das Dokument unbedingt verinnerlichen, denn sie müssen den Jugendlichen diesbezüglich ggf. Rede und Antwort stehen. Dazu reicht es nicht aus, die 10 Punkte an sich auflisten zu können, sondern auch zu verstehen, warum die einzelnen Punkte gut sind. Dieses Verständnis gilt es dann auch, den jugendlichen Internetbenutzern beizubringen. Sie müssen wiederum Kenntnis vom Dokument genommen haben und ihren Willen geäußert haben, sich an die Regeln zu halten, bevor ihnen der Zugang zum Computer gewährt wird. Das betreuende Personal muss in diesem Rahmen dafür sorgen, dass jedem jugendlichen Benutzer im Vorfeld eine Kopie des Dokuments ausgehändigt wird.

1.3. Privatgebrauch am Arbeitsplatz

Die Erzieher dürfen die im Jugendhaus zur Verfügung gestellten Computer mit Internetzugang für private Zwecke nutzen, solange diese Nutzung nicht gegen die Sicherheitsregeln verstößt oder sie dadurch ihr Pflichten als Betreuer vernachlässigen. Die Erzieher bewegen sich in der Regel relativ barrierefrei in der für sie vorgesehenen Netzzone „Betreuungspersonal“. Jedoch gilt auch für sie: Illegale Aktionen, wie zum Beispiel das Herunterladen von Musik oder Programmen auf Filesharing-Portalen sind tabu!

Der private Gebrauch von Internet und Computer darf unter keinen Umständen zu einer Störung der Arbeitsabläufe im Jugendhaus führen. Weder die Arbeit des betreffenden Erziehers noch die seiner Kollegen darf darunter leiden.

1.4. Gebrauch des informatischen Systems

Computer und Internet im Jugendhaus dürfen nicht für unlautere Zwecke missbraucht werden. Das beinhaltet jegliche Aktionen, die anderen Personen, Instanzen oder dem Jugendhaus selbst Schaden zufügen könnten. (Cyber)mobbing, Rufschädigung oder Verleumdung fallen ebenfalls in diese Kategorie.

Wie in Punkt 1.2.1 des Leitfadens für den OZ beschrieben wird, hat jeder Mitarbeiter im Jugendhaus lediglich Zugriff auf die Daten und Informationen, die er zum korrekten Ausführen seiner Arbeit braucht. Sein Aktionsraum ist auf diese Daten und Informationen beschränkt, es sei denn, er erhält vom OZ eine Ausnahmeerlaubnis zum Lesen, Kopieren, Zerstören, Umändern oder Kopieren weiterer Daten.

Die Erzieher verpflichten sich dazu, das zur Verfügung gestellte Material mit Sorgfalt zu benutzen und aufzubewahren, so dass einem vorzeitigen Verschleiß vorgebeugt wird.

1.5. Umgang mit Passwörtern

Das Passwort, Basiselement der Informationssicherheit, erlaubt die eigene Identifikation und den Zugriff auf persönliche Ressourcen und Dienste. Es ist unbedingt notwendig, dass sich das Betreuungspersonal über ein starkes Passwort in seinen Computer und in das Netzwerk loggt. Jeder Mitarbeiter muss sich ein eigenes, starkes Passwort ausdenken.

Ein solches **starkes Passwort** ist wie folgt zusammengesetzt:

- Regelmäßig (mindestens einmal im Jahr) geändert
- Aus mindestens 10 Zeichen bestehend (es sei denn, das System beschränkt die Anzahl der Passwort-Zeichen, wie etwa bei einem Pin-Code aus 4 Zahlen)
- Mindestens Groß- und Kleinbuchstaben sowie Zahlen (bestenfalls auch Sonderzeichen) enthaltend

Der Erzieher ist persönlich verantwortlich für den Schutz seines Passworts. Es ist ihm strengstens untersagt:

- Provisorisch vergebene Passwörter nach dem ersten Einloggen weiter zu benutzen. Das Passwort muss beim ersten Einloggen sofort erneuert werden, da provisorische Passwörter oft nicht den Sicherheitsbestimmungen entsprechen und sehr leicht zu erraten sind.
- Leicht zu erratende Passwörter zu benutzen (eigener Name, Name des Haustiers, ein Geburtsdatum, eine Telefonnummer, ein Wort aus dem Wörterbuch, usw.). Solche Passwörter können sogar von nicht-professionellen Hackern leicht erraten werden. Spezielle Computerprogramme benötigen nur wenige Sekunden, um Passwörter zu knacken, die Elementen bestehen, die im Wörterbuch zu finden sind.
- Das gleiche Passwort für mehrere Anwendungen zu benutzen. So ist der Schaden, falls ein Passwort abhandenkommt, umso verheerender.
- Sein Passwort an eine andere Person weiterzugeben oder zu verraten. Ein Passwort ist persönlich und geheim. Gibt man es weiter, hat man keine Kontrolle mehr über seine Nutzung oder eventuellen Missbrauch.
- Sein Passwort per Telefon, E-Mail oder sonstige Internetverbindung mitzuteilen. Diese Kommunikationswege sind nicht sicher. Das Passwort könnte abgefangen und für unlautere Zwecke missbraucht werden.
- Das Passwort so aufzuschreiben, dass es nicht ausreichend geschützt ist. Dass Passwörter nicht arglos in der Nähe des Computers aufgeschrieben sein sollten (etwa auf ein Post-it notiert und an den Bildschirm geklebt), versteht sich von selbst. Insgesamt wird stark davon abgeraten, Passwörter niederzuschreiben. Muss man es

dennoch tun, sollte man sie chiffrieren. Zu diesem Zweck gibt es auch spezielle Computerprogramme, wie zum Beispiel Keepass (keepass.info). Hier werden Passwörter verschlüsselt in einer sicheren Datenbank abgespeichert, die per Masterpasswort versiegelt wird.

1.6. Umgang mit dem elektronischen Material

Den Erziehern wird im Jugendhaus ein Computer zur Verfügung gestellt. Dies bringt einige Verantwortung mit sich. So ist der Erzieher verpflichtet:

- Den Zugang zu seinem Computer per Passwort zu schützen
- Seinen Computer zu blockieren, bzw. in den Standby-Modus zu versetzen (der nur per Passworteingabe freigeschaltet werden kann), wenn er seinen Arbeitsplatz verlässt, auch wenn dies nur für einen kurzen Moment ist. Der Erzieher hat die Pflicht, Dokumente und Informationen, die sich auf seinem Computer befinden, zu schützen. Aus diesem Grund muss der Zugriff durch Außenstehende unter allen Umständen verhindert werden.
- Keine Downloads von Programmen oder anderen Dateien an seinem Arbeitsplatz vorzunehmen. Es sei denn, er hat vorher die Erlaubnis des operationellen Zuständigen (OZ) eingeholt.
- Alle Dokumente, an denen er arbeitet, sorgfältig in seinem Computer abzuspeichern. Das bezieht sich nicht auf regelmäßige Backups der gesamten Dateien, sondern lediglich auf das reguläre Abspeichern von Projekten. Dieses sollte für alle Benutzer informatischer Systeme ein Standardreflex sein.

1.7. Gebrauch von Webdiensten

Das Secure-MJ-Gehäuse beinhaltet einen Internetfilter, der an die verschiedenen Benutzerzonen angepasst werden kann. Problematische Inhalte, die auch in der Zone „Betreuungspersonal“ generell blockiert werden sind Pädophilie, Rassismus, Verleumdung, Gewaltverherrlichung und solche, die anderen Menschen Schaden zufügen können oder aus einem anderen Grund als illegal eingestuft werden. Stellt ein Erzieher fest, dass solch problematischen Inhalte dennoch zugänglich sind, also durch den bestehenden Filter gerutscht sind, muss er den OZ darüber informieren. Dieser wird den Internetfilter ggf. anpassen.

Aufgepasst bei Downloads aus dem Internet! Sind sie illegal, missachten sie geltende Autorenrechte oder könnten sie dem EDV-System schaden (hinter vielen Downloads aus dem Internet verbirgt sich Schadsoftware), dürfen sie auf keinen Fall getätigt werden. Im Zweifelsfall sollte die Meinung und ggf. die Erlaubnis des OZ eingeholt werden, oder der Download abgebrochen werden.

Urheberrecht: Was ist erlaubt?

Urheberrechtlich geschützte Werke darf man sich in der Regel ansehen oder anhören, so oft man will. Erlaubt ist es außerdem: Für den privaten Gebrauch Musik- und TV-Sendungen aufzunehmen, CDs und legale Downloads zu kopieren (sofern sie keinen Kopierschutz haben), oder sich Dokumente aus dem Internet herunterzuladen. Solche Privatkopien dürfen

allerdings nur im engen Freundes- und Familienkreis konsumiert werden. Solange kein wirksamer Kopierschutz dabei umgangen wird, darf man auch CDs auf den Computer oder MP3-Player überspielen, oder für einen Freund oder ein Familienmitglied einen Sampler mit verschiedenen Songs zusammenstellen.

Für den privaten Gebrauch ist es ebenfalls erlaubt, Internetradio aufzunehmen oder Videos aus Mediaportalen (z.B. YouTube) zu speichern. Man darf im Internet auch Filmausschnitte verwenden, Produktfotos und Screenshots von anderen Medien veröffentlichen, sofern man sie als Zitate kenntlich macht und die Quelle angibt. Das Gleiche gilt für das Zitieren fremder Texte.

Urheberrecht: Was ist verboten?

Sobald etwas im Internet veröffentlicht wird, ist es nicht mehr nur für den privaten Gebrauch, sondern kann Millionen von Menschen erreichen und potenziell gewerbliche Zwecke verfolgen. Deshalb darf man Werke, auch wenn man sie legal erworben hat, nicht ins Internet hochladen, und schon gar nicht auf Tauschbörsen zum illegalen Download anbieten. Genauso darf man keine gekauften CDs oder Computerprogramme kopieren, um sie anschließend im großen Rahmen zu verteilen oder sogar zu verkaufen. Wer eine eigene Webseite betreibt, oder sein Internetprofil, Blog, oder ähnliches mit fremden Texten, Fotos, Musik, oder Videos bereichern möchte, muss vorher die ausdrückliche Erlaubnis des Urhebers einholen. Ansonsten drohen teure Abmahnungen!

Legal ist sicherer

Viele Dateien in Peer-to-Peer-Netzwerken sind nicht das, wofür sie sich ausgeben: hinter verlockenden Namen können sich unerwartete Inhalte verstecken (z.B. pornografisches oder pädopornografisches Material).

Illegale Downloads beinhalten oft Viren, Würmer oder andere böswillige Programme und sollten deshalb vermieden werden.

Wer Autorenrechte nicht respektiert, und geschützte Inhalte wie Musik oder Filme im Internet teilt, beziehungsweise herunterlädt, macht sich strafbar.

Neben all den illegalen Möglichkeiten, gibt es immer noch eine Reihe von Gratis- und Bezahlplattformen, die es ermöglichen, ohne Risiken von diesen Werken zu profitieren. Sie sind die sicherere Alternative!

1.8. Der Umgang mit E-Mail

Auch im Umgang mit E-Mail müssen die Erzieher einige Regeln beachten:

- Dateianhänge sollten in geregelten Maßen verschickt werden
- Beim Erhalt von E-Mails ist Skepsis geboten. Bei zweifelhaften E-Mails kann es sich um Betrugsmaschen oder Spam handeln. Im schlimmsten Fall können sich in Mail-Anhängen oder unter angebotenen Links sogar Viren und andere Schadprogramme verstecken. Im Zweifelsfall sollten E-Mails besser ignoriert und vernichtet werden.

- Niemals auf Spam antworten: Wenn Sie Spam beantworten, oder durch den dafür vorgesehenen Button abbestellen möchten, weiß der Absender, dass Ihre Adresse aktiv ist und wird weiterhin (noch mehr) unerwünschte Mails darauf senden.
- Niemals vertrauliche Informationen aufgrund einer E-Mail preisgeben: Seriöse Organisationen würden niemals vertrauliche, persönliche oder Zugangsdaten zu Verbindungen (Passwörter) anfordern, insbesondere nicht per E-Mail. Im Zweifelsfall kann man versuchen, sich mit dem Absender der Mail direkt in Verbindung zu setzen.
- Nicht auf Links in E-Mails klicken, ohne vorher die Vertrauenswürdigkeit der Quelle überprüft zu haben: Diese Links leiten oft auf gefälschte (wenn auch täuschend echt aussehende) Webseiten weiter, auf denen Ihre Daten gespeichert und anschließend für unlautere Zwecke missbraucht werden.
- E-Mail ist kein sicheres Kommunikationsmittel und eignet sich somit nicht zum Versenden vertraulicher Mitteilungen. Ein Dritter kann mit einfachen technischen Mitteln auf den Inhalt der Korrespondenz zugreifen. Lässt es sich nicht vermeiden, vertrauliche Informationen per E-Mail zu verschicken, sollte man eine Chiffriertechnik anwenden, um die Nachricht zu schützen.

Folgende Handlungen sind sowohl innerhalb als auch außerhalb des Jugendhauses untersagt:

- Das Versenden von Spam oder Ketten-E-Mails.
- E-Mails mit Inhalten, die durch das luxemburgische Gesetz verboten sind. Zum Beispiel das Verteilen von internen Fotos oder vertraulichen Daten.
- Jeglicher Missbrauch des E-Mail-Systems, der die Sicherheit des informatischen Systems bedrohen und den Ruf des Jugendhauses schädigen könnte. Zum Beispiel das Versenden von Schadprogrammen oder rufschädigenden Nachrichten.

Was ist Spam?

Spam sind Nachrichten mit meist werbendem Inhalt, die man ungewollt über E-Mail erhält. Für viele Internetbenutzer ist Spam eine echte Plage, denn die Nachrichten wollen von Diätprodukten über Potenzmittel bis hin zu Billigreisen so ziemlich alles an den Mann bringen und überschwemmen das E-Mail-Konto regelrecht mit oft Dutzenden Nachrichten am Tag. Darüber hinaus sind sie eine nicht zu unterschätzende Gefahrenquelle, denn nicht selten übermitteln sie Schadprogramme, oder es handelt sich um Phishing-Mails, die private Daten ausspionieren möchten. Weiteres Risiko: Wird Spam beantwortet, weiß der Absender, dass die betreffende Adresse noch gültig ist, und versendet daher weiterhin unerwünschte Mails.

Was sind Ketten-E-Mails?

Bei Ketten-E-Mails handelt es sich um E-Mails, die schnellstmöglich an eine bestimmte Zahl von Bekannten weitergeleitet werden sollen, unter dem Vorwand, dass sonst zum Beispiel etwas ganz Schlimmes passiert ("Wenn du diese Mail nicht innerhalb von 24 Stunden an 24 Freunde weiterschickst, wird jemand, den du liebst sterben!!") oder mit dem Versprechen, dass dann ein Wunder passiert ("Wenn jeder, der diese Nachricht erhält, sie an mindestens 10 Personen weiterschickt, wird dieses kranke Kind 100.000 Euro für seine lebensrettende OP bekommen!"). Diese Nachrichten entsprechen in keinem Punkt der Wahrheit und sollten

nicht weitergeleitet werden. Die Schicksale die darin beschrieben werden, sind frei erfunden. Man sollte sie einfach ignorieren und löschen.

1.9. Aufgeräumter Arbeitsplatz und Entsorgung von Dokumenten

Wechseldatenträger oder Papierdokumente mit vertraulichen Informationen dürfen nicht unbeaufsichtigt am Arbeitsplatz liegen gelassen werden. Zu groß ist die Gefahr, dass eine unbefugte Person Zugriff darauf erhält.

Genauso sollte darauf geachtet werden, Papiere mit sensiblen Daten schnell aus Druckern, Fax- und Kopiergeräten zu entfernen.

Werden Dokumente nicht mehr benötigt, sollten sie fachgerecht entsorgt werden. Dabei reicht es nicht aus, sie einfach in den Papierkorb zu verschieben. Denn was gemeinhin als „Löschen" bezeichnet wird, bedeutet bloß eine Entfernung der Datei aus dem Index. Sie kann dann nicht mehr per Betriebssystem gefunden werden. Ihr Inhalt bleibt jedoch auf dem Datenträger bestehen und könnte mithilfe des richtigen Programms mit wenig Mühe wiederhergestellt werden. Aus diesem Grund ist es unbedingt notwendig, den Speicherplatz einer sensiblen Datei mit neuen Inhalten zu überschreiben, so dass ihr ehemaliger Inhalt nicht wieder lesbar gemacht werden kann. Dazu gibt es spezielle Löschprogramme, wie etwa „CCleaner"[6] oder „Eraser"[7], die man sich gratis im Internet herunterladen kann.

Auch Dateien auf Wechseldatenträgern kann man auf diese Art löschen. Will man den Datenträger nicht wieder benutzen, besteht auch die Möglichkeit, ihn physisch, durch Krafteinwirkung (kaputt machen oder verbiegen) funktionsuntüchtig zu machen. Papierdokumente sollten selbstverständlich geschreddert werden.

1.10. Gesetzgebung befolgen

Es wird vorausgesetzt, dass jeder Erzieher die Gesetzestexte kennt und anwendet, die für seine Arbeit und insbesondere den Umgang mit Minderjährigen relevant sind.

Es ist strengstens untersagt, die Speicherfunktion des Secure-MJ-Kastens zu missbrauchen, um das Surfverhalten von Personen zu rekonstruieren, bzw. zu überwachen. Dies würde gegen geltende Bestimmungen für den Schutz von Daten und Privatsphäre verstoßen und wäre dementsprechend strafbar.

In diesem Rahmen müssen die Gesetze bezüglich des geistigen Eigentums vom 18. April 2001[8] und bezüglich der privaten Daten vom 2. August 2002[9] allen Erziehern bekannt sein.

[6] Über den Hersteller: http://www.piriform.com/ccleaner
[7] Über den Hersteller: http://eraser.heidi.ie/
[8] *Loi du 18 avril 2001 sur les droits d'auteur, les droits voisins et les bases de données.*
[9] *Loi du 2 août 2002 relative à la protection des personnes à l'égard du traitement des données à caractère personnel.*

1.11. Sanktionen

Zuwiderhandlungen der in dieser Charta beschriebenen Regeln und der geltenden Gesetze, seien sie einmalig oder wiederholt, können bestraft werden und rechtliche Konsequenzen mit sich ziehen.

4.1.3 BEE SMART
Verhaltensregeln für das Jugendhaus

Die SMART-Regeln sollen den jugendlichen Besuchern im Jugendhaus einen gewissenhaften Umgang mit Computer und Internet nahebringen. Der operationelle Zuständige (OZ) muss dafür sorgen, dass die Erzieher dieses Dokument genau kennen. Sie müssen nämlich sicherstellen, dass die Jugendlichen es gesehen haben und seinen Inhalt verstehen, bevor sie den Computer benutzen. Am besten geschieht dies, indem die Regeln gut sichtbar in der Nähe der Computer angebracht werden. Außerdem sollte jeder, der zum ersten Mal einen Computer im Jugendhaus benutzt, diese Regeln individuell erklärt bekommen. Die Jugendlichen müssen im Vorfeld ihren Willen geäußert haben, sich daran zu halten, bevor ihnen Zugang zum Computer gewährt wird. Es liegt in der Verantwortung der Erzieher, den Jugendlichen zu erklären, was diese Regeln sind, und warum es wichtig ist, sie zu respektieren.

S für „Sicherheit“

- Passwörter geheim halten
- Downloads und Installationen nur mit Erlaubnis des Erziehers

M für „Misstrauen“

- Nicht alles, was im Internet steht, ist wahr. Deshalb gilt:
  Kettenbriefe und Spam ignorieren, Quellen prüfen, nicht auf fragwürdige Anhänge und Links klicken
- Nicht mit Leuten treffen, die man nur aus dem Internet kennt

A für „Achtsamkeit“

- Keine persönlichen Infos auf dem Computer abspeichern
- Aus Webdiensten richtig ausloggen
- Sorgsam mit dem zur Verfügung gestellten Material umgehen

R für „Respekt“

- Urheberrechte respektieren (gilt für alle Inhalte, also Bilder, Texte, Filme,…)
- Keine illegalen Downloads (Musik, Videos,…) machen
- Rassistische und gewaltverherrlichende Webseiten sind tabu
- Immer höflich bleiben
- Recht auf Privatsphäre respektieren

T für „Teile mit!“

- Mobbing schnellstmöglich melden
- Bei Problemen oder Fragen an einen Erzieher wenden
- Anonyme Beratung und Hilfe gibt es telefonisch bei der BEE SECURE Helpline

Am Ende des Dokuments steht der an die Jugendlichen gerichtete Verweis:

„Mir ist bewusst, dass alles, was ich im Internet tue, zurückverfolgt werden kann und dass ich für meine Online-Aktivitäten verantwortlich bin.“

Diese Grundregeln, in Form eines Plakats gestaltet, sind beim SNJ jederzeit nachbestellbar.

Im Jugendhaus haben die Besucher die Möglichkeit, kostenlos einen Computer mit Internetzugang zu nutzen. Dabei handelt es sich um hochwertige Geräte, deren Finanzierung vom Familienministerium oder in einzelnen Fällen von der Gemeinde oder Sponsoren übernommen wird. Den Jugendlichen sollte vermittelt werden, dass es sich dabei nicht um eine unerschöpfliche Quelle handelt. Im Gegenteil: Kommt es zu Vandalismus oder mutwilliger Beschädigung, muss damit gerechnet werden, dass ein kaputtes Gerät nicht ersetzt wird. Den Jugendlichen sollte darüber hinaus der Respekt vor fremdem Eigentum beigebracht werden. Ein wichtiger Schritt, um die Jugendlichen mit in die Verantwortung einzubeziehen, besteht darin, sie zu ermuntern, Anomalien, Defekte und sonstige Auffälligkeiten sofort zu melden. Das alles zum Wohl „ihrer“ Computer.

Alle Programme, die zum Arbeiten am Computer und Surfen im Internet benötigt werden, sind bereits auf dem Gerät installiert. Es ist also normalerweise nicht nötig, weitere Programme zu installieren. Möchte ein Jugendlicher dies trotzdem tun, benötigt er das Einverständnis des operationellen Zuständigen (OZ).

Bei der Installation von Programmen muss darauf geachtet werden, dass es sich um legale und lizenzierte Ausgaben handelt. Bei Downloads aus dem Internet ist Vorsicht geboten: Oft versteckt sich dahinter eine Schadsoftware.

Die Computer im Jugendhaus sind allen Besuchern zugänglich. Den Jugendlichen muss deshalb mitgeteilt werden, dass alle Dokumente, die sie dort abspeichern, theoretisch für andere einsehbar sind. Besser ist es deshalb, zum Beispiel mit Wechseldatenträgern wie USB-Sticks zu arbeiten. Außerdem wichtig: Sich aus Webdiensten stets durch den dafür vorgesehenen Button ausloggen. Wer nur die Seite schließt, ohne sich richtig abzumelden, riskiert dem nächsten Benutzer Zugriff auf seine Dienste zu gewähren.

Die Erzieher sollten für die Jugendlichen stets Ansprechpartner sein. Besonders auch, wenn es um Fragen bezüglich Computer, Internet und neue Medien geht. Diese spielen eine wichtige Rolle im Leben der Jugendlichen. Es versteht sich also von selbst, dass auch die Erzieher sich diesbezüglich informieren und weiterbilden sollten, um angemessene Ansprechpartner zu sein.

Teil 3: BEE SECURE im Jugendhaus

4.2 Praktische Animationen

BEE SECURE steht den Jugendhäusern als begleitender Partner im Bereich der Computer- und Informationssicherheit zur Seite.

Bei interaktiven Schulungen und Workshops besucht ein BEE SECURE Trainer das Jugendhaus und macht sich ein Bild über die Internetgewohnheiten der Jugendlichen, indem er sie z.B. direkt darauf anspricht, wie sie ihre Zeit am Computer verbringen. Auf diesen Erkenntnissen gründet der Ablauf der modular aufgebauten Präsentation. Je nachdem, wo die Interessen der Jugendlichen liegen, geht der Trainer dann mehr auf spezifische Themen ein. Ziel ist es, in einer lockeren Atmosphäre zu Diskussionen und Meinungsaustausch anzuregen.

Der Trainer hat im Jugendhaus die Möglichkeit, Animationen mit den Jugendlichen durchzuführen. So können wichtige Inhalte besser visualisiert werden. Um die Jugendlichen zum Mitmachen anzuregen und ihnen wertvolle Tipps auf anschauliche und interaktive Weise zu vermitteln, bieten sich eine Menge Aktivitäten an.

Solche Sensibilisierungsaktionen können beim SNJ angefragt werden:

Tel: 247-86400
www.bee-secure.lu/form

Auch Erzieher können diese eigenständig, ohne dass dafür die Präsenz eines BEE SECURE Trainers notwendig wäre, durchführen. Auf den folgenden Seiten werden Animationsbeispiele aufgelistet.

4.2.1 Diskussionseröffnung

„Was macht ihr im Internet?“

Jugendliche erzählen von ihren Aktivitäten, von besonderen Erfahrungen und ihrer Einstellung gegenüber den neuen Medien. Ein aktuelles Thema (wie seinerzeit z.B. ACTA, Anonymous o.ä.) bietet sich gut als Diskussionsgrundlage an.

Wahrscheinlich wird diese Einführung in die Diskussion relativ lange dauern. Jugendliche erzählen gerne und viel von ihren eigenen Erfahrungen und stellen bereits hier Fragen, die später noch einmal aufgegriffen und vertieft werden können.

Die Diskussionseröffnung dient dazu, Schwerpunkte für anschließende Aktivitäten zu setzen.

4.2.2 Aktivitäten zum Thema Selbstdarstellung im Netz – Privatsphäre

„Molekül“

Material: Papier und Kugelschreiber
Zeit: ca. 15 Min.

Jeder Teilnehmer (inkl. Trainer) erhält ein Blatt und einen Kugelschreiber und soll sich als Molekül grafisch darstellen. Ein kleiner Kreis (Atom) bildet den Anfang und wird mit dem eigenen Namen versehen. Weitere Atome (Kreise) werden angedockt und stellen die eigenen Interessen und Aspekte dar, die eine wichtige Rolle im eigenen Leben spielen: „Was macht dich aus?“.

Wenn alle fertig sind, soll jeder überlegen: „Gibt es ein Atom, das nicht online zu sehen sein sollte?“ Besprechung in der Runde: Hierdurch soll deutlich werden, dass es einen Unterschied geben sollte zwischen der eigenen Darstellung in der Onlinewelt und in der Realität und dass man genau überlegen sollte, was man online preisgibt, also veröffentlicht. Nicht alle Aspekte, die einen selber ausmachen, gehören ins Internet. Bsp.: kranke Oma spielt eine sehr große Rolle im eigenen Leben, man kümmert sich sehr um sie und verbringt viel Zeit mit ihr, ist traurig, dass es ihr nicht mehr so gut geht. Ein wichtiger Aspekt des eigenen Lebens, der aber nicht unbedingt öffentlich breitgetreten werden sollte.

„Peinliche Situation“

Material: ---
Zeit: ca. 20-30 Min.

Die Teilnehmer sollen sich Situationen in Erinnerung rufen, die sehr peinlich waren. Ob sie diese der Gruppe mitteilen, oder für sich behalten möchten, ist ihnen selbst überlassen. Daraus entsteht ein Gespräch darüber, wie es wäre, wenn diese Situationen online konserviert wären und wie gut es ist, dass Dinge vergessen werden können.

„Warum ist mein Ruf mir wichtig?“

Material: ---
Zeit: ca. 15-30 Min.

Es wird darüber diskutiert, warum es wichtig ist seinen Ruf zu wahren und warum man Angst hat, einen guten Ruf zu verlieren. Der Zweck einer positiven Reputation sollte erkannt werden. Hier kann auch wieder auf das „Molekül“ verwiesen werden.

„Reputations-Check“

Material: Computer mit Internetzugang
Zeit: ca. 15 Min.

Die eigene Online-Reputation definiert sich über folgende Inhalte im Internet:

- Eigene Inhalte
- Inhalte über eigene Aktivitäten
- Von anderen generierte Inhalte

Falls Internetzugang vorhanden ist, sollten die TeilnehmerInnen herausfinden, was im Internet über die eigene Person zu finden ist. Steht Unvorteilhaftes bei der Google-Suche an erster Stelle? Was kann dagegen unternommen werden? Die Teilnehmer loggen sich bei http://takethislollipop.com ein und schauen sich den Film an. Vorher muss mit dem Erzieher abgeklärt werden, ob der Inhalt evtl. problematisch sein könnte für einzelne Teilnehmer. Anschließend wird die Wirkung auf die Teilnehmer besprochen.

Die Wichtigkeit des regelmäßigen Checkens der Suchergebnisse über eigene Person (sich selber googeln) sollte erkannt werden. Jeder kann seine Online-Reputation beeinflussen. Man kann sich bspw. eine eigene URL anlegen, unter der positive Aspekte zu finden sind. Man sollte sich um sein Online-Ich kümmern und dieses regelmäßig checken und ggf. säubern.

4.2.3 Aktivitäten zum Thema Bilder im Internet (Recht am eigenen Bild – Copyright)

Polaroid-Aktion

Material: Polaroid-Kamera mit genügend Filmen (Kann von BEE SECURE über den Service National de la Jeunesse zur Verfügung gestellt werden), Themenblatt „Recht am eigenen Bild“
Zeit: ca. 20 Min.

Diese Aktion kann durch eine direkte Frage eingeläutet werden: „Kennt ihr Polaroid-Kameras?“ oder „Wer möchte ein Polaroid-Foto haben?“. Der Erzieher macht dann ein Foto von einem Teilnehmer und stellt, während das Bild sich entwickelt, die Frage: „Was ist das Besondere an diesem Foto?“. Die Antwort: „Dieses Foto hast du unter deiner Kontrolle. Du

alleine kannst entscheiden, was mit ihm passiert, solange es in deinem Besitz ist. Das Bild ist ein Unikat, und nicht auf dem Fotoapparat gespeichert."

Dann wird die Frage aufgeworfen, ob man das gleiche auch von der modernen, digitalen Fotografie behaupten kann, beziehungsweise von Bildern, die online gepostet werden. Den Jugendlichen wird während der Diskussion bewusst, dass, sobald ein Bild im Internet ist, es ohne ihr Wissen in Sekundenschnelle manipuliert und vervielfältigt werden kann. Die Devise lautet „einmal im Netz – immer im Netz". Und Kontrolle hat man darüber keine.

Während der Aktion erhält jeder Teilnehmer ein Polaroid-Porträtfoto von sich als Erinnerung. Dazu gibt es eine Kopie des BEE SECURE Themenblatts „Recht am eigenen Bild"[10]. Die Jugendlichen sollten zur Erkenntnis gelangen, dass es besser ist, sich zweimal zu überlegen ob und welche Bilder man ins Netz stellen sollte. Dabei sollte auch angesprochen werden, dass man erst die Erlaubnis von den darauf abgebildeten Personen einholen muss, ehe man ein Foto publizieren darf. Außerdem hat jeder, der ein Bild von sich im Internet findet, mit dem er nicht einverstanden ist, das Recht, dessen Entfernung zu verlangen. Weitere Infos diesbezüglich befinden sich auf dem Themenblatt.

4.2.4 *Aktivitäten zum Thema Informationen im Internet*

„2 Sender berichten"

Den Jugendlichen werden nacheinander zwei verschiedene Berichterstattungen aus dem Internet zu ein und demselben Thema gezeigt. Danach sollen innerhalb einer Diskussion die Unterschiede herausgearbeitet werden. Der Fokus liegt darauf, den Jugendlichen zu zeigen, wie weit belegbare Informationen und Annahmen oder gar Wertungen auseinander liegen können. Zudem sollen sie dazu angeregt werden, das Gesehene / Gehörte kritisch zu verarbeiten und eventuell selbst nochmals zu überprüfen. Ein sehr geeignetes Beispiel hierfür ist die Berichterstattung zur Gamescom aus dem Jahr 2011. Als wohl bekanntestes Negativ-Beispiel kann hier nämlich die Berichterstattung von RTL[11] gelten, die aufgrund der darin geäußerten Demütigungen und dem Mangel an Informationen stark in die Kritik geriet. Als Gegenbeispiel kann der Bericht von Phoenix[12] dienen.

Ziel der Aktivität ist es, den Jugendlichen zu zeigen, wie wichtig eine gesunde Portion Skepsis beim Surfen im Internet ist. Das WWW steckt voll von Meinungen, Fakten und Pseudo-Wissen. Profitieren kann man davon, wenn man mehrere Quellen vergleicht und dabei den eigenen kritischen Sinn nicht ausschaltet.

„Facebook – Persönliche Einstellungen"

Die meisten Jugendlichen sehen kein Problem darin, Privates für Freunde und sogar Fremde bei Facebook zugänglich zu machen. Sie schätzen die möglichen Folgen von zu viel Öffentlichkeit und unüberlegter Datenfreigabe falsch ein. Generell gilt: je mehr Daten

[10] https://www.bee-secure.lu/sites/default/files/BEE%20SECURE%20-%20bildrecht_DE-Recht%20am%20eigenen%20Bild.pdf
[11] http://www.youtube.com/watch?v=WcI7wyXQ9U0
[12] http://www.youtube.com/watch?v=bFiP0EFSZc4&list=PL5FA388A1B22EB023

öffentlich zugänglich sind, desto angreifbarer macht man sich. Daher sollte genau überlegt sein, welche persönlichen Einblicke man preisgibt und welchem Personenkreis. D.h. insbesondere für Facebook-Mitglieder: persönliche Einstellungen überprüfen und Änderungen der Facebook-Konditionen verfolgen.

An dieser Stelle kann das Youtube-Video „Wir wollen dich doch nur kennenlernen“ über den (kaum vorhandenen) Schutz der Privatsphäre bei Facebook gezeigt werden[13].

Anschließend kann eine Diskussion entstehen, bei der darauf eingegangen wird, wie Facebook sein Geld verdient. Angesprochen werden z.B. personalisierte Werbung, persönliche Daten, Datenausbeutung, Möglichkeiten der maschinellen Datenverarbeitung usw.

Ideal ist es, wenn sich die Erzieher aktiv mit den Jugendlichen auseinandersetzen und ihnen helfen, ihre Privatsphäre-Einstellungen bei Facebook zu konfigurieren. Dafür könnte eine Art Workshop organisiert werden.

4.2.5 Aktivität zum Thema Cybermobbing

„Gefühlsbarometer“

Das „Gefühlsbarometer“ kann das Jugendhaus über BEE SECURE beziehen. Es handelt sich um Situationskärtchen und eine dazu passende Bewertungsskala.

Bei dieser Aktivität erhalten alle Teilnehmer ein oder mehrere Kärtchen, die eine unangenehme Situation beschreiben (z.B. „beim Chat mit der Webcam wirst du aufgefordert, dein T-Shirt auszuziehen“, „jemand rempelt dich absichtlich an“ oder „du erhältst jeden Tag eine SMS wo drin steht „du bist doof und niemand kann dich leiden“). Diese Kärtchen gilt es dann, verdeckt auf das Gefühlsbarometer zu kleben, und zwar auf einer Skala von 0 („finde ich nicht verletzend“) bis 10 („das verletzt mich sehr“). Hat jeder seine Karten an die für ihn passende Stelle auf der Skala abgelegt, wird das Gesamtwerk umgedreht.

Hier wird dann deutlich, wie unterschiedlich die gleichen Situationen von verschiedenen Personen bewertet werden. Was die einen als nicht tragisch empfinden, ist für die anderen oft ein schwerer Schlag und umgekehrt.

Kernaussage: Respektiere die Gefühle des Anderen. Was du witzig findest, darüber kann der andere vielleicht gar nicht lachen. Im richtigen wie im virtuellen Leben muss man seine Mitmenschen respektieren, um ein friedliches Miteinander zu schaffen.

[13] http://www.youtube.com/watch?v=e4re7mwQzIA

4.3 Weiterbildung

Kein Medium ist so dynamisch und entwickelt sich so rasend schnell weiter, wie das Internet. Wollen Erzieher kompetente Ansprechpartner für die Jugendlichen sein, ist es essenziell, dass sie sich regelmäßig auf den neusten Wissensstand bringen. Deshalb empfiehlt BEE SECURE die Weiterbildung der Erzieher im Bereich der Medienerziehung. Entsprechende Angebote sind auf dem Weiterbildungsportal enfancejeunesse.lu angegeben.

Im Weiterbildungskatalog werden jedes Jahr mehrere Weiterbildungen angeboten. Sie sind mit dem BEE SECURE-Logo hervorgehoben.