

Protokoll der Sitzung „Sicherheit und Konsumentenschutz“

Zeit: 26.5.2008, 9:00-13:00

Ort: RTR-GmbH, Mariahilfer Straße 77-79, 1060 Wien

1 Management Summary

Ziel dieser öffentlichen Veranstaltung war, die Ergebnisse der ersten Sitzung auf einer breiten Basis zu erörtern, neue Perspektiven zu gewinnen und weitere Vorschläge zu sammeln. Das vorliegende Ergebnisprotokoll gibt die Statements und Vorschläge der TeilnehmerInnen in verdichteter Form wieder, wobei das Redaktionsteam selbstverständlich alle mündlichen und schriftlichen Äußerungen und Maßnahmenvorschläge gesichert hat. Im gegenständlichen Management Summary wird ein Auszug aus den Ergebnissen dargestellt, wobei die stattgefundenen Diskussionen nur in stark komprimierter Form wiedergegeben werden können.

Im Themenfeld „E-Business“ sprechen sich die ExpertInnen für eine stärkere Promotion bestehender Gütesiegel aus, warnen aber vor einer Inflation von Gütesiegeln. Bezüglich der schwarzen Liste stellen die ExpertInnen fest, dass diese für inländische Unternehmen als effektiv gelten, aber nicht für ausländische. Die ExpertInnen würden leicht verständliche Rechtsinformation und -beratung für die KonsumentInnen begrüßen. Außerdem erachten die ExpertInnen eine Harmonisierung der Rechtsnormen für wichtig, insbesondere im Bereich Konsumentenschutz.

Im Themenfeld „Illegale Inhalte / Kinder- und Jugendschutz“ halten die ExpertInnen fest, dass es bereits einige Initiativen gibt. Zudem wird betont, dass die beiden Themenbereiche nicht miteinander vermischt werden dürfen und man auch zwischen illegalen und unerwünschten Inhalten unterscheiden muss. Da illegale Inhalte ein internationales Problem sind, sollte nach Meinung der ExpertInnen versucht werden, zumindest innerhalb der EU eine Vereinheitlichung herbeizuführen. Die ExpertInnen erachten die Sensibilisierung der Kinder und Jugendlichen hinsichtlich des Umgangs mit persönlichen Daten in sozialen Netzwerken für äußerst wichtig. Auch würden sie eine (durchgehende) Klassifizierung von Inhalten für nützlich halten. Grundsätzlich sprechen sich die ExpertInnen für eine bessere Vermittlung des Medienverständnisses aus, indem Elternvereine verstärkt eingebunden werden oder ein IT-Beauftragter pro Sprengel/Bezirk eingesetzt wird. Auch können Schulprojekte, in denen die Schüler Inhalte selbst produzieren, forciert werden, um das Medienverständnis zu fördern.

Ein zentraler Punkt, der im Arbeitskreis „Netzintegrität“ angesprochen wurde, ist, dass eine breite Vertrauensbasis unter den Usern und Unternehmen Voraussetzung dafür ist, dass Sicherheitsprobleme rasch und unbürokratisch gelöst werden können. Es muss ein Informationsaustausch auf lokaler, nationaler und internationaler Ebene stattfinden. Das österreichische CERT soll ausgebaut werden und eine aktive Teilnahme der Stakeholder wird gefordert. Es wird festgestellt, dass dieses Thema in weiteren Arbeitskreisen vertieft werden muss.

Im Themenfeld „Datenschutz“ empfehlen die ExpertInnen, das Bewusstsein über das „lange Gedächtnis“ des Internets und das Hinterlassen von Spuren zu stärken. Dies könnte in Form

von Awareness- und Aufklärungskampagnen erfolgen. Insbesondere bei der Jugend und bei der älteren Generation ist dieses Bewusstsein nach Meinung der ExpertInnen nur gering ausgeprägt. In diesem Zusammenhang könnten Friendly Internet Kurse für diese Zielgruppen angeboten werden. Als weitere Maßnahme begrüßen die ExpertInnen einen Lösungsanspruch, sofern dieser technisch realisierbar wäre. Einige ExpertInnen votieren bei der gewerblichen Weitergabe der Daten für eine Opt-In Regelung. Die ExpertInnen sprechen sich dafür aus, dass Unternehmen ihre Kundendaten den Behörden nur aufgrund eines richterlichen Beschlusses aushändigen sollen. Allgemein wird appelliert, bei legislativen Maßnahmen im Bereich Datenschutz die Stakeholder zu Rate zu ziehen.

Im Arbeitskreis „Computersicherheit“ wird festgestellt, dass nur informierte User sicher im Netz unterwegs sind. Um dies gewährleisten zu können, muss IT-Sicherheit als fixer Bestandteil in der Aus- und Weiterbildung verankert werden. Der niederschwellige Zugang zu dieser Thematik ist besonders wichtig. Im Fokus soll außerdem eine diesbezügliche Ausbildung der Lehrerschaft sein. Ein wesentlicher Eckpfeiler bezüglich der Computersicherheit ist auch die Bewusstseinsbildung. Außerdem sollen IT-Sicherheitschecks forciert werden. In Anlehnung an das KFZ-Pickerl soll ein solches auch für die Computersicherheit verwendet werden. Servicestellen für PCs sollen geschaffen werden, die eventuelle Risiken, welche auf den Rechnern bestehen, auflisten und Lösungsvorschläge geben.

2 Allgemeines

Auf Grundlage der Ergebnisse der 1. Sitzung hat am 26.5.2008 die 2. Sitzung (Public Event) zum Arbeitskreis „Sicherheit und Konsumentenschutz“ in den Räumlichkeiten der RTR-GmbH stattgefunden. Ziel war es, die Ergebnisse der ersten Sitzung auf einer breiten Basis zu erörtern, neue Perspektiven zu gewinnen und weitere Vorschläge zu sammeln. In einer dritten und letzten Sitzung werden die gesamten Ergebnisse gesichtet, vorliegende Maßnahmen priorisiert und damit Schwerpunkte für den Draft der Internet-Deklaration festgelegt.

Das Redaktionsteam hat die mündlichen und schriftlichen Statements und Vorschläge der TeilnehmerInnen gesichert und gibt diese im vorliegenden Ergebnisprotokoll in verdichteter Form wieder. Der Fokus dieses Protokolls liegt nicht darin, sämtliche Einzelaussagen als vielmehr konkrete Vorschläge und übereinstimmende Aussagen wiederzugeben, wobei freilich alle Äußerungen der TeilnehmerInnen durch die Protokollführer dokumentiert sind. Die Inputs der TeilnehmerInnen werden vom Redaktionsteam weder bewertet noch priorisiert, sondern nur gesammelt und geordnet.

3 Zum Prozess

Nach einer Präsentation ausgewählter Vorschläge der ExpertInnen aus der ersten Arbeitskreissitzung wurden die TeilnehmerInnen aufgerufen, die offenen Punkte zu diskutieren und neue Vorschläge zu unterbreiten. Zu diesem Zweck konnten die TeilnehmerInnen im ersten Block an einer von drei parallel laufenden Subgruppen zu den Themen „E-Business“, „Illegale Inhalte / Kinder- und Jugendschutz“ und „Netzintegrität“ teilnehmen und im zweiten Block an einer der Subgruppen zu den Themen „Datenschutz“ und „Computersicherheit“ mitarbeiten. In diesen Subgruppen wurden unter Anleitung eines Moderators die Themen diskutiert und Vorschläge erarbeitet. Jeder Teilnehmer / jede Teilnehmerin hatte außerdem die Möglichkeit, schriftlich zum Thema Stellung zu beziehen. Danach stellte jeweils ein Teilnehmer / eine Teilnehmerin aus einer Subgruppe im Plenum eine kurze Zusammenfassung vor.

4 Die Ergebnisse

Die TeilnehmerInnen wurden aufgefordert, basierend auf den Ergebnissen der ersten Sitzung im Wesentlichen über folgende Themen zu diskutieren:

1. „E-Business“,
2. „Illegale Inhalte / Kinder- und Jugendschutz“
3. „Netzintegrität“
4. „Datenschutz“ und
5. „Computersicherheit“

Die Ergebnisse werden nachfolgend für jedes Thema gesondert dargestellt, wobei zu jedem Thema die unterbreiteten Vorschläge und gemachten Aussagen angeführt und diese punktuell zum Verständnis und zur näheren Erläuterung skizziert werden. Die Diskussion über die vorgeschlagenen Maßnahmen sowie die anderen Details sind vom Redaktionsteam intern festgehalten und fließen ebenso in die dritte Arbeitskreissitzung ein.

4.1 E-Business

a. Gütesiegel ausbauen

- Die ExpertInnen betonen die Bedeutung von Gütesiegeln, die den Konsumenten garantieren, dass die Leistung/das Produkt zumindest getestet wurde. Manche ExpertInnen halten das Führen einer weißen Liste für sinnvoller als das einer schwarzen Liste.
- Die ExpertInnen sprechen sich für eine stärkere Promotion bestehender Gütesiegel aus, gleichzeitig sind Vorkehrungen zu treffen, damit es nicht wie im Lebensmittelbereich zu einer Inflation von Gütesiegeln kommt.
- Ein weiteres Problem sehen die ExpertInnen auch darin, dass zwar Portalbetreiber ein Gütesiegel verwenden können, dies aber nicht für die Subunternehmer gilt.

b. Awareness für die schwarze Liste stärken

- Die ExpertInnen weisen daraufhin, dass es von der Europäischen Verbraucherzentrale bereits eine Alert Liste gibt und auch der Internet-Ombudsmann eine Watchlist führt.
- Aus den Erfahrungen der Watchlist hat sich gezeigt, dass ein Großteil der gelisteten Unternehmen ausländische sind. Bezüglich der inländischen Unternehmen wird die schwarze Liste als effektiv gesehen, die Unternehmen sind bestrebt, einen Eintrag zu vermeiden.
- Die ExpertInnen schlagen vor, das Bewusstsein der Konsumenten zu stärken und sie dazu zu motivieren, vor Vertragsabschluss diese Liste zu konsultieren.
- Die Möglichkeit der Gewinnabschöpfung wird von einigen ExpertInnen nicht als effizientes Instrument gesehen, insbesondere wenn das betroffene Unternehmen im Ausland sitzt. Einige ExpertInnen sprechen sich für die Gewinnabschöpfung aus, da damit ein wichtiges disziplinierendes Instrument vorhanden wäre, um Unternehmen zu einem rechtskonformen Verhalten zu bringen.

c. Bessere Rechtsinformation und -beratung für Konsumenten, KMUs und EPU's

- Im Internet fehlt im Gegensatz zum Kauf im Geschäft der persönliche Kontakt zwischen Käufer und Verkäufer sowie die Information unter welche Rechtsvorschriften das gegenständliche Rechtsgeschäft fällt. Daher forcieren die ExpertInnen leicht verständliche Rechtsinformation und -beratung für die KonsumentInnen. Insbesondere soll transparent gemacht werden, wer der Vertragspartner ist.

d. Schaffung von einheitlichen Rechtsnormen auf hohem Niveau in Europa

- Aufgrund des grenzüberschreitenden Handels sind die Unternehmen auch als Einkäufer mit verschiedenen Rechtsnormen unterschiedlicher Länder konfrontiert. Daher erachten die ExpertInnen eine Harmonisierung der Rechtsnormen als wichtig.
- Insbesondere betreffend dem Konsumentenschutz drängen die ExpertInnen auf eine Vereinheitlichung, wobei sie davor warnen, nicht nur die Mindeststandards durchzusetzen. Konkret würden sie Bemühungen um eine einheitliche Musterrücktrittsbelehrung als vorrangig erachten.
- Einige ExpertInnen weisen daraufhin, dass die Rechtsdurchsetzung bei grenzüberschreitenden Aktivitäten bereits durch eine Verordnung zur Behördenkooperation vorgesehen ist. Die zuständige Behörde eines Anbieterlandes wird vom Missbrauch informiert und aufgefordert, den Missbrauch abzustellen. Einige ExpertInnen meinten, dass in der Praxis kaum Ressourcen der Behörden für solche Fälle vorhanden sind, sodass diese Verordnung ins Leere geht.

e. Vertragsrücktritt/Vorleistungen Rücktrittsbedingungen verbessern und vereinfachen

- Einige ExpertInnen sprechen sich dafür aus, dass KonsumentInnen für den Kauf im Internet keine Vorleistung zu leisten haben sollen und dass die Regeln über das Rücktrittsrecht effizienter gestaltet werden sollten.
- Einige ExpertInnen halten dagegen, dass es auch unter den KonsumentInnen einen geringen Anteil gibt, der die Ware erhält und diese nicht bezahlt. Dieser Gruppe darf man den Missbrauch nicht erleichtern.

4.2 Illegale Inhalte / Kinder- und Jugendschutz

Eingangs wird von den ExpertInnen festgehalten, dass es zu den beiden Fragen „illegale Inhalte“ und „Kinder- und Jugendschutz“ bereits einige Initiativen gibt. Angemerkt wird auch, dass die Diskussionen dazu beispielsweise in Deutschland bereits weiter fortgeschritten sind. Zudem wird festgehalten, dass die beiden Themenbereiche nicht miteinander vermischt werden dürfen (z.B. legale pornografische Inhalte vs. Kinderpornografie vs. Kinder- und Jugendschutz) und man auch zwischen illegalen und unerwünschten Inhalten unterscheiden muss.

a. Illegale und unerwünschte Inhalte

- Illegale Inhalte sind ein internationales Problem (teilweise sind Inhalte in einem Land zulässig, in einem anderen nicht). Es sollte nach Meinung der ExpertInnen daher versucht werden, zumindest innerhalb der EU eine Vereinheitlichung herbei zu führen. In der Diskussion scheint dies aber problematisch, da es nicht einmal eine einheitliche Werthaltung innerhalb der EU gibt.

b. Sensibilisierung über Folgen der Internetnutzung

- In Bezug auf Kinder und Jugendliche sind es meist nicht illegale Inhalte, die Grund zur Sorge geben, sondern (legale) Inhalte, die für Kinder und Jugendliche nicht geeignet sind.
- Sensibilisierung hinsichtlich des Umgangs mit persönlichen Daten: Soziale Netzwerke boomen, und Kinder und Jugendliche geben hier oft sehr viel an persönlichen Informationen weiter, ohne die Folgen abschätzen zu können. So kann ein Foto einer geselligen Runde zu Jugendzeiten noch als Spaß interpretiert werden, bei einem späteren Bewerbungsgespräch aber schon mal Erklärungsbedarf auslösen.
- In diesem Zusammenhang wird von den ExpertInnen kurz das Thema „Löschung“ von Daten im Internet angesprochen. Dies ist aber nicht primäres Thema dieses Themenfeldes.
- Grundsätzlich besteht immer der Reiz des Verbotenen (gerade im jungen Alter). Verlockung kann nicht unterbunden werden. In diesem Zusammenhang wird die Frage der Sperre von einzelnen Seiten/Angeboten diskutiert. Eine solche erscheint aber schwierig, da es zu einem Katz-und-Maus-Spiel mit den Jugendlichen bzw. den Betreibern von Webseiten ausarten würde. Generell muss man bei dem Thema „Sperre von Inhalten“ aufpassen, dass man nicht in den Bereich der Zensur rutscht.
- Eine Lösung könnte die (durchgehende) Klassifizierung von Inhalten sein. Damit könnten dann auch wirksame Filter installiert werden, die Kindern und Jugendlichen bestimmte Angebote im Internet nicht mehr zugänglich machen.
- Derartige Klassifizierungssysteme gibt es teilweise bereits heute, jedoch meist auf freiwilliger Basis. Gütesiegel (E-Commerce) ICRA / ICRA checked (privater Verein in UK)

- „Die Geister die ich rief“ – Web 2.0.: Die Fülle an Inhalten wird/ist unüberschaubar, sodass schon auch deshalb eine durchgehende Klassifizierung als sehr schwierig erscheint.
- Kurz angedacht wurde auch, die Schaffung spezieller Seiten für Kinder und Jugendliche zu forcieren.

c. Medienverständnis fördern:

- Ein Problem scheint den ExpertInnen die Forderung zu sein, „Eltern und LehrerInnen in die Pflicht zu nehmen“, ohne sich zu überlegen, was dies bedeutet. Wie soll etwas vermittelt werden, von dem man selbst keine oder nur wenig Ahnung hat? In diesem Zusammenhang merken die ExpertInnen an, dass das Schulsystem nicht als einziges/wichtigstes Element gesehen werden kann.
- Als mögliche Maßnahme wird eine verstärkte Einbindung der Elternvereine (Schaffung von Medienkompetenz) angedacht. Auch sollte die Einsetzung von IT-Beauftragten pro Sprengel/Bezirk gefördert werden.
- Die ExpertInnen fordern, dass zunehmend auch Inhalte von Schülern im Rahmen des Unterrichts bzw. von Projekten selbst produziert werden, um das Medienverständnis weiter zu fördern (wie entstehen Inhalte, welche Beteiligten wirken hier mit, usw.). In diesem Zusammenhang wurde auch angemerkt, dass es bereits einige sehr fortschrittliche Schulen gibt. Die ExpertInnen schlagen vor, anhand von Best-Practice-Beispielen auf solche Projekte aufmerksam zu machen bzw. diese durch Wettbewerbe zu fördern.

d. Generelles Angebot an Informationen für Kinder und Jugendliche über den Umgang mit dem Internet.

- Die Nutzung des Internets wird in den Lehrplänen bereits forciert (Beschaffung von Informationen). Hier wäre nach Meinung der ExpertInnen eine Information der Schüler bereits im Vorfeld wichtig (wie gehe ich mit Inhalten um, wie können Inhalte bewertet werden, welche „Gefahren“ lauern im Internet, usw.).
- Positiv wird herausgestrichen, dass es umfangreiche Initiativen in Österreich gibt, die sich mit diesem Thema auseinandersetzen. Als möglicher Problempunkt wird von den ExpertInnen aufgeworfen, dass viele der vorhandenen Informationsbroschüren zu umfangreich sein könnten und daher oftmals nicht gelesen werden.
- Eine Maßnahme nach Ansicht der ExpertInnen könnten auch Aufklärungskampagnen unter dem Motto „Aufklärung ist der beste Schutz“ in den Medien (Fernsehen und Hörfunk) sein.

e. Infrastruktur verstärken

- Als Problem wird von den ExpertInnen auch die fehlende Infrastruktur gerade in den Bundesländern kritisiert („Österreich besteht nicht nur aus Wien“). Hier müssen Maßnahmen gesetzt werden, die eine flächendeckende Versorgung mit Infrastruktur in den Bildungseinrichtungen gewährleisten (ist auch Thema im Lebensbereich Infrastruktur).

4.3 Netzintegrität

a. Web of Trust errichten

- Die ExpertInnen sind der Meinung, dass eine stärkere Vertrauensbasis unter den Usern (Unternehmen, Internet Providern, Behörden,...) geschaffen werden sollte,

damit Sicherheitsprobleme rasch und unbürokratisch gemeldet werden. Diese Vertrauensbasis muss auch zu internationalen Stellen aufgebaut werden. Viele Unternehmen/Personen melden Vorfälle nicht, weil sie im Fall von Computerkriminalität auf das Polizeikommissariat gehen und dort persönlich Anzeige erstatten müssten. Diese Hürde kann abgebaut werden, indem über ein Webportal Sicherheitsprobleme anonym gemeldet werden können.

- Dieses Webportal kann auch einen Informationsaustausch auf allen Ebenen, nämlich international, national und lokal ermöglichen. Damit schafft man Strukturen, die einen Informationsaustausch über Sicherheit und Probleme erlauben. Aufklärungsarbeit bezüglich der Problemerkennung soll stärker geleistet werden, da dies der erste Schritt ist.
- Konkret schlagen die ExpertInnen vor, Guidelines betreffend Netzintegrität für KMUs herauszugeben. Nach Ansicht der ExpertInnen könnte diese Integrität durch ein diesbezügliches Gütesiegel dokumentiert werden. Dazu sollten die Betreiber mit einbezogen werden. Dies könnte in Form eines Sicherheitshandbuches erfolgen.
- Die ExpertInnen regen an, dass im Verfassungsschutzbericht den IKT eine bedeutendere Rolle zukommt.
- Allgemein wird festgestellt, dass Sicherheit zwar Geld kostet, ein Nichtimplementieren aber im Zweifelsfall teurer werden kann, wenn dadurch großer Schaden entsteht.

b. Ausbau CERT (Computer Emergency Response Team)

- Es wird festgestellt, dass Österreich Schlusslicht bezüglich des CERT ist. Es weiß zwar jeder, dass Kommunikationsinfrastruktur wichtig ist, aber niemand will Geld in die Hand nehmen. Weder die Definition einer kritischen Infrastruktur noch die in einer Krisensituation zu ergreifenden Maßnahmen sind geklärt.
- Deshalb empfehlen die ExpertInnen, CERT unter aktiver Teilnahme aller Beteiligten (Stakeholder) auszubauen. Nach Meinung der ExpertInnen braucht es dazu ein „lokales“ österreichisches Sicherheitssystem. Dieses soll in 5 Schritten arbeiten:
 1. Sensoring: Früherkennung
 2. Monitoring: Beobachtung von „Vorläufer“-Aktivität
 3. Verification: Korrelation, Aggregation von Bedrohungsbildern, korrekte rasche Beurteilung
 4. Response: Koordinierte Abwehrmaßnahmen
 5. Coordination: national und international (Abgleich mit anderen Expertensystemen)
- Dazu soll nach Ansicht der ExpertInnen ein Sensornetzwerk in Österreich errichtet und der regelmäßige Informationsaustausch zwischen Infrastrukturbetreibern sichergestellt werden.
- Die ExpertInnen waren sich nicht einig, ob das CERT zentralistisch aufgebaut werden sollte und ob der Schwerpunkt im öffentlichen Sektor liegen soll.
- Es wird darauf hingewiesen, dass die Möglichkeit zum hoheitlichen Eingreifen vorhanden sein sollte. Dazu sollten nach Ansicht der ExpertInnen Strukturen errichtet werden, um Attacken gegen kritische Infrastrukturen zu verifizieren und zu überprüfen, damit auch effektive Gegenmaßnahmen eingeleitet werden können.

c. Internationale und nationale Kooperation stärken

- Bedrohungen der Netzinfrastruktur können nur mit nationalen und internationalen Kooperationen begegnet werden. Dazu ist es notwendig, Informationen über den Zustand der Netze und über sicherheitsbedrohliche Notfälle zu sammeln. Eine zentrale Koordination und zentrale Empfehlungen sind für die Netzintegrität notwendig, eine international koordinierte Kommunikation und Zusammenarbeit ist Voraussetzung.

- Es wird festgestellt, dass dieses Thema in weiteren Arbeitskreisen vertieft werden muss.

4.4 Datenschutz

a. Schutz der Nutzer vor sich selbst ist zu stärken

- KonsumentInnen sind sich nicht bewusst, dass das Internet ein „langes Gedächtnis“ hat und diese Archivierung durch die Vernetzung verstärkt wird. Außerdem hinterlassen KonsumentInnen – selbst wenn sie keine eigenen Inhalte ins Internet stellen oder Informationen bekannt geben – Spuren.
- Die ExpertInnen betonen, dass das Bewusstsein dafür durch Awareness- und Aufklärungskampagnen gestärkt werden sollte. Insbesondere bei der Jugend und bei der älteren Generation ist dieses Bewusstsein nach Meinung der ExpertInnen nur gering ausgeprägt. In diesem Zusammenhang könnten Friendly Internet Kurse für diese Zielgruppen angeboten werden, die über bestimmte Sicherheitsverhaltensweisen aufklären. Auch können bestehende Initiativen ausgebaut werden, um sie einer größeren Zielgruppe zugutekommen zu lassen
- Als weitere Maßnahme begrüßen die ExpertInnen einen Lösungsanspruch, sofern dieser technisch realisierbar ist. Damit soll den KonsumentInnen das Recht gegeben werden, ihre Inhalte zu löschen.
- Außerdem sind die ExpertInnen der Meinung, dass das Bewusstsein für Anonymisierungssysteme gestärkt werden soll.

b. Schutz der Nutzer vor Unternehmen, die die Daten gewerblich verwerten, ist zu stärken

- Die ExpertInnen sprechen sich für eine Einschränkung der Weitergabe von Daten an Dritte aus. Einige ExpertInnen votieren für eine Opt-In Regelung bei der Weitergabe von Daten, d.h. der Kunde muss ausdrücklich der Weitergabe zustimmen, wobei eine Zustimmung zu den AGB-Klauseln alleine dafür nicht reichen darf. Einige ExpertInnen weisen darauf hin, dass derzeit Unternehmen das gewerbliche Nebenrecht zur Weiterverwendung der Daten mit Zustimmung des Kunden haben. Freilich sollen Unternehmen, die ihren Kunden Leistungen anbieten, die für das Anbieten der Leistungen erforderlichen Daten erhalten.
- Im Bezug auf die gewerbliche Nutzung öffentlicher Daten meinten einige, dass die Unternehmen kostenfrei auf diese Daten zugreifen können sollten. Auf der anderen Seite gab es Bedenken, dass damit öffentliche Daten über BürgerInnen verknüpft werden können und der Datenschutz der BürgerInnen nicht gewährleistet wäre.

c. Schutz der Nutzer vor Staat (Grundrechte) ist zu stärken

- Die ExpertInnen sprechen sich dafür aus, dass Unternehmen ihre Kundendaten den Behörden nur aufgrund eines richterlichen Beschlusses aushändigen müssen. Kritisiert wird das Sicherheitspolizeigesetz, in dem die Begehrlichkeiten der öffentlichen Hand nach Meinung der ExpertInnen sehr ausgeprägt sind.
- Die Novelle, die die Abschaffung des Datenschutzes bei juristischen Personen vorsieht, wird von einigen ExpertInnen abgelehnt. Auch die Verpflichtung, einen Datenschutzbeauftragten für Unternehmen ab 20 Mitarbeitern zu benennen, wird abgelehnt. Allgemein wird appelliert, bei legislativen Maßnahmen im Bereich Datenschutz keine Schnellschüsse zu wagen, sondern die Stakeholder und ExpertInnen zu Rate zu ziehen.

- Ein Experte nennt folgendes Beispiel als Illustration für die Probleme im Datenschutz. Bei der Vernetzung von 1200 Bildungseinrichtungen mittels Plattformen Fragen zum Datenschutz aufgetaucht sind, für die keine rechtlich haltbare Rechtsposition eingeholt werden konnte. Das Datenschutzrecht kann Hemmschwelle für diese innovativen Applikationen sein. Die Rechtsnormen sollten jedenfalls nicht der Intensivierung der Internet Nutzung entgegenstehen.

d. Datenschutz als nicht IKT-spezifisches Thema

Einige ExpertInnen weisen darauf hin, dass es sich um ein gesellschaftlich-kulturelles Thema handelt, dass Daten unabhängig vom Internet gesammelt werden und es daher kein internet-spezifisches Thema ist.

4.5 Computersicherheit

a. IT Sicherheitsverkehrserziehung - Nur informierte User sind sicher im Internet

- Nach Ansicht der ExpertInnen sollte die IT-Sicherheitsausbildung genau so grundlegend und dauerhaft wie Verkehrserziehung durchgeführt werden. Dies muss als Grundlagenwissen bereits in Kindergärten und Schulen thematisiert werden.
- Zusätzlich soll die IT-Sicherheit als fixer Baustein in Aus- und Weiterbildungsprogramme wie z.B. den ECDL-Computer-Führerschein integriert werden.
- Die IT-Bildung muss laut den ExpertInnen (noch) „niederschwelliger“ werden. Dies kann z.B. in Form von sog. „Beipackzetteln“, die bei Abschluss eines Providervertrages und/oder Computerkauf beigegeben werden, passieren. Dieser soll einige wenige wichtige Informationen beinhalten und Verweise auf Webseiten enthalten, von denen kostenlose und kostenpflichtige Tools heruntergeladen werden können.
- Die Frage der Ausbildung scheint am wichtigsten zu sein. Hier muss nach Ansicht der ExpertInnen ein systematischer Prozess stattfinden, der bei den LehrerInnen starten muss. Die LehrerInnen sollten jedenfalls motiviert werden, hier tätig zu werden.
- Es gibt derzeit einen „Split“ zwischen: „Ich habe ein Problem“, und: „Ich tue etwas dagegen“. Diese Diskrepanz muss geschlossen werden. Dies kann nur mit ausreichender Kommunikation erfolgen.
- Österreich ist ein Staat der „Ein-Personen-Unternehmen“. Es sollen sog. „Sicherheitsbausteine“ vor allem für kleinere Unternehmen angeboten werden, die dann auch von Mitarbeitern der Firma privat genutzt werden dürfen. Diese Sicherheitsbausteine sollen sowohl kostenlose als auch kostenpflichtige Tools wie Firewalls, Virenschutz etc. beinhalten.

b. Laufende Bewusstseinsbildung

- Die Bewusstseinsbildung wird von den ExpertInnen als ein wesentlicher Eckpfeiler zur Erhöhung der Computersicherheit gesehen. Vor allem im Bildungsbereich (bei Ausbildung von Schülern, Pädagogen, und Erwachsenenbildung) sollte IT-Sicherheit thematisiert werden. Das Ziel ist es, ein breites Bewusstsein zu schaffen.
- Aufgrund der freien und unzensurierten Verfügbarkeit des Internets ist die Kompetenz in der Entscheidungsfindung zu stärken, wobei Einschränkungen in Abhängigkeit zu Risiken und Notwendigkeiten zu sehen sind. Entmündigung bzw. Zensur darf nicht stattfinden.
- „Durch Schaden wird man klug.“ Es wird eine Art Haftpflichtversicherung für Computer diskutiert. Wenn ein Grundset an Sicherheitstools nicht genutzt wird, soll

ev. Schadenersatz gefordert werden können. Aufklärung ist zu wenig, es soll sanfter Druck ausgeübt werden.

- Für den ECDL-Computerführerschein ist Computersicherheit derzeit kein Thema. Dies muss sich rasch ändern. Es gibt von der OCG Bildungsmaterial, auch dieses ist aber nicht im ECDL integriert.

c. Sicherheitchecks forcieren - Der unsichere Computer von heute ist mein Schadensfall von morgen

- Es sollen nach Ansicht der ExpertInnen PC-Security-Check Seiten regelmäßig aufgerufen werden müssen. Es wird diskutiert, ein so genanntes „Pickerl“ (in Anlehnung an das KFZ-Pickerl) für Computersicherheit einzuführen. So soll Bewusstsein für Computersicherheit geschaffen werden.
- Wie beim Auto sollen sog. „Servicestellen“ für PCs geschaffen werden, die eventuelle Risiken, welche auf dem Rechner bestehen, auflisten und Lösungsvorschläge geben.
- Die ExpertInnen stellen fest, dass es derzeit ein Problem mit nicht vorhandenen Standards für Computersicherheit gibt. Diese ist aufgrund der heterogenen Umgebung auch sehr schwer zu definieren. Jedoch könnte es ein standardisiertes Sicherheitspaket für BürgerInnen geben.
- Jedenfalls müssen sog. „Standardempfehlungen“ wie z.B.: Updates für Virenschutzsoftware herunterladen, Firewall installieren etc. vermehrt kommuniziert werden. Hier stellt sich die Frage, wie man dies dem Kunden bestmöglich vermittelt. Es wird vorgeschlagen, dem Konsumenten ein Best-Practice-Beispiel an Sicherheitsregeln leicht und niederschwellig zu kommunizieren.