Schriftenreihe
Nr. 71

Cyber Security Summit

Jugend im Cyberspace – Security als Schlüsselwort

4. Dezember 2012, HTL Rennweg

OVE GIT Informations- und Kommunikationstechnik

CYBER SECURITY SUMMIT
der Gesellschaft für Informations- und Kommunikationstechnik (GIT) im OVE

JUGEND IM CYBERSPACE – SECURITY ALS SCHLÜSSELWORT

LIZ (Lern- und Informationszentrum) der HTL Rennweg, Wien

4. Dezember 2012

Impressum

Herausgeber: Gesellschaft für Informations- und Kommunikationstechnik (GIT) im OVE
Verlag: Österreichischer Verband für Elektrotechnik (OVE)
Satz: Ulrike Haring

ISBN 978-3-85133-077-9

Eschenbachgasse 9 | 1010 Wien
www.ove.at

Band 71 der OVE-Schriftenreihe

Fotos: Sergey Nivens, Vladislav Kochelaevs - fotolia.de

INHALTSVERZEICHNIS

1 Begrüßung

durch Dipl.-Ing. **Helmut LEOPOLD**
Präsident OVE-GIT, AIT Austrian Institute of Technology,
Head of Department Safety & Security

Jede neue Technologie beeinflusst die Nutzer und vice versa, so Helmut Leopold bei der Begrüßung zum ersten „Cyber Security Summit", der am 4. Dezember 2012 im Lern- und Informationszentrum der HTL Rennweg über die Bühne ging. Und je mehr Technik wir einsetzen, um die größten anstehenden Probleme der Menschheit zu lösen, desto mehr sind wir auf jene gigantischen Kommunikationsinfrastrukturen angewiesen, die uns heute zur Verfügung stehen. Der rasant wachsende Cyber-Raum bietet aber nicht nur Chancen, sondern ist auch Risken ausgesetzt, mit denen sich Wirtschaft, Wissenschaft, Politik und Gesellschaft verstärkt konfrontiert sehen.

Da insbesondere die Jugendlichen als „digital natives" zu den Hauptakteuren des Cyberspace gehören, ist die Schaffung von Bewusstsein und Awareness für den verantwortungsvollen Umgang mit den neuen Medien ein vordringliches Anliegen, dem sich dieser „Cyber Security Summit" stellt. Industrie, Meinungsbildner, Politiker und Bildungsverantwortliche sind daher gefordert, den sicheren Umgang mit dieser neuen Kulturtechnik in ihren Zukunftsstrategien angemessen zu berücksichtigen. „Cyber Security" muss Teil der Bildung und Ausbildung werden und sichere Kommunikationstechnologien bleiben das oberste Ziel, wenn wir die elektronische Vernetzung unserer Kinder und Jugendlichen künftig so gefahrlos wie möglich gestalten wollen.

Auch wenn wir als Erziehergeneration, als „digital immigrants", weniger vom Umgang mit neuen sozialen Medien verstehen wie unsere Kinder, so haben wir doch die Verantwortung, sie sicher durch die „always-on"-Welt zu begleiten. Unsere Nachkommen erwarten sich das auch geradezu von uns.

Der heutige „Cyber Security Summit" bringt daher Fachleute und Jugendliche zusammen, um gemeinsam über ein brandheißes Thema aus unterschiedlichsten Blickwinkeln zu betrachten und zu diskutieren. Als Präsident der OVE-GIT, der diesen Gipfel veranstaltenden Gesellschaft für Kommunikations- und Informationstechnik im Österreichischen Verband für Elektrotechnik, bleibt mir noch allen TeilnehmerInnen einen angeregten Erfahrungsaustausch und viele neue Einsichten am Ende des Tages zu wünschen.

2 Einleitung und Eröffnungsvortrag „Jugend im Cyberspace"

Dipl.-Ing. **Thomas BLEIER,** MSc., AIT Austrian Institute of Technology, Safety & Security Department, Thematic Coordinator ICT Security

Thomas Bleier, der in der OVE-GIT, die Arbeitsgruppe „Cyber Security" leitet, führte nicht nur durch die Veranstaltung, sondern hielt auch einen eigenen Eingangsvortrag zum Thema „Jugend im Cyberspace". Sein Tenor zur derzeitigen Situation lautete: „Für die Infrastrukturen der Zukunft wird IKT-Sicherheit eine Kernkomponente sein – die Jugend von heute wird in den nächsten Jahren als Benutzer und auch als Entwickler und Betreiber dieser Infrastrukturen fungieren. Daher ist es wichtig, schon frühzeitig Awareness für Sicherheitsthemen zu schaffen, um sowohl Risiken als auch Chancen und Lösungswege zu diskutieren."

Bleier führte in die Thematik damit ein, indem er die Rasanz der Veränderungen im IT-Zeitalter an Hand der Durchdringungsdauer einzelner Technologien eindrucksvoll demonstrierte. Mit der Frage „wie lange es gedauert hat, dass 50 Millionen Benutzer eine bestimmte Technologie verwenden", wird sehr schnell klar, dass der Zeitraum für das Erreichen dieser Coverage mit Fortgang der Technologieentwicklung immer kürzer wurde. Während die Zeitung, das gedruckte Wort, nach Erfindung der Buchpresse noch ungefähr 100 Jahre, also 4 Generationen benötigte um auf 50 Millionen Leser zu kommen, sich die Verbreitung der Elektrizität im Hinblick auf zeitweise unsichere Technik und sich hartnäckig haltende Vorbehalte auch aus der wissenschaftlichen Welt sowie durch die ländlichen Siedlungsmuster in zB den USA noch über 70 Jahre, also drei Generationen hinzog, brauchte das Automobil nur mehr 50 Jahre oder zwei Generationen bis zum Durchbrechen der 50 Millionen Nutzer-Schallmauer.

Mit dem Eintritt ins Medienzeitalter geht es dann zunehmend zügiger. Das Erreichen von 50 Millionen Radiozuhörern dauerte immerhin noch 38 Jahre, Fernsehen benötigte nur noch 13 Jahre, das Internet gerade mal 4 Jahre, das Smartphone 2 ½ Jahre und die Social Media heutigen Zuschnitts nur noch 2 Jahre.

Die Reihe lässt sich für Applikationen und Plattformen mühelos fortsetzen, das Tempo der Durchdringung bei den Nutzern nimmt weiter zu. Facebook benötigte noch 852 Tage, bis 10 Millionen das soziale Medium nutzten, Twitter mit 780 Tagen etwas weniger und g+ (Google Plus) durchbrach diese Grenze in sagenhaften 16 Tagen.

Thomas Bleier führte in seinem Vortrag weiter aus, dass Cyber-Security heute einer Vielfalt von Herausforderungen gerecht werden muss. So verlangen z.B. die Vernetzung aller Geräte, die Auslagerung von Anwendungen und Programmen in die Cloud sowie das immer stärker im Berufsalltag Fuß fassende „BYOD" (Bring Your Own Device) Konzept und die damit einhergehende Consumerization, eine durchgängig an den Bedürfnissen der Konsumenten ausgelegte Spielart der IT-Nutzung sowie die zahllosen Interaktionen in Social Networks und Social Media nach völlig neuen und verbesserten Security-Ansätzen. Gerade diese revolutionären Entwicklungen bei der Gestaltung des „digitalen Lebens" mit Mitteln moderner IKT haben im großen Stil auch Cybercrime- und Cyberwar-Aktivitäten zusätzlichen Antrieb gegeben.

In Zukunft werden sich die Bedrohungen aus dem Cyberspace wie die Einschleusung von Schadprogrommen (Trojaner, Spyware, Würmer etc.) oder Phishing (z.B. Identitätsklau) noch verschärfen, weil wir den Großteil unserer Informationen bereits durch IKT-Systeme aufbereitet und gefiltert erhalten werden. Beispiele dafür sind Google, Siri, Wikipedia oder YouTube und es wird uns in einer „always on, always connected"-Welt auch zunehmend schwerer fallen, die Suchergebnisse auf ihre Richtigkeit oder ihren Wahrheitsgehalt bzw. ihre Authentizität zu prüfen. Wir gehen schnellen Schrittes auf eine Gesellschaft zu, in der Informationen nur gesucht und nicht mehr gespeichert werden und in der sich virtuelle und physische Realitäten miteinander vermischen.

Mit diesem Lagebild verändern sich auch die Motivlagen für Angriffe aus dem Web. Galt für Hacking oder Cracking bislang vielfach auch das Prinzip, aus Spaß Sicherheitslücken beweisen zu wollen, wird Cybercrime wie zB. Phishing künftig zunehmend finanziellen Motiven folgen und die Sicherheitsschwachstellen gezielt für Attacken bei Online Banking, Web-Dienstleistungen oder Urheberrechtsverletzungen nutzen. Institutionelle Attacken mit entsprechender Manpower und finanzieller Ausstattung aus der Gattung Cyberterrorism und Cyberwar könnten aber noch viel größere Schäden in unserer Netz-basierten Wissensgesellschaft anrichten, indem sie wichtige Infrastrukturen wie z.B. Energienetze oder urbane Verkehrssysteme lahmlegen und damit unsere modernen Kulturen an ihrem zentralen Lebensnerv treffen.

Thomas Bleier argumentiert, dass es überall dort Incentives für Hacking gibt, wo auch ein Markt gegeben ist. Das betrifft z.B. digitale Medien und Applikationen wie die DVD, das SatTV, die Playstation, das iPhone und Chiptuning für Autos, aber auch Phishing und Zero-Day Black Markets, wo Angriffstools für auch dem Hersteller von Software noch nicht bekannte Sicherheitslücken versteigert werden. Technologisch gesehen sind für Bleier die Werkzeuge im Prinzip die gleichen, egal ob damit eine Kreditkarte oder private Daten gestohlen werden, oder ein Atomkraftwerk gehackt wird.

Der Security-Experte des AIT untermauerte seine Ausführungen mit einem sehr drastischen Beispiel aus dem Online-Magazin „Wired“, der Story des dortigen Redakteurs Mat Honan, dem durch Folgeverkettung all seiner Accounts auf Apple, Amazon, Google und Twitter bei einem Hackangriff mit einem Schlag sein gesamtes „digitales Leben“ ausgelöscht worden ist. Honan nutzte Apple‘s Cloud Service „iCloud“ für iPhone Backup und Synchronisierung. Der Zugang zur Apple ID ist durch ein Passwort gesichert. Das Rücksetzen dieses Passwortes kann über Apple Support durch Bekanntgabe der Rechnungsadresse und der letzten 4 Ziffern der Kreditkarte erfolgen. Honan hat aber auch einen Amazon-Account. Hier kann ein Hacker anrufen und unter Vorgabe einer falschen Identität angeben, dass er eine neue Kreditkarte hinzufügen möchte. Dafür braucht er Accountname, E-Mail und Rechnungsadresse – alles Angaben, die von professionellen Hackern unschwer zu eruieren sind. Danach ruft der Hacker nochmals den Amazon Support an und erklärt, dass er den Zugang verloren hat. Mit Account, Rechnungsadresse und einer zuvor hinzugefügten, gefaketen Kreditkartennummer kann er eine neue E-Mail-Adresse hinzufügen. Damit kann der Phishing-Täter das Passwort zurücksetzen, hat Zugriff auf den Account und sieht letzten Ziffern der zuletzt benutzten Kreditkarten. Mit diesen hat dann auch Zugriff auf den iCloud Account und auf alle Apple-Devices des Opfers.

Thomas Bleier wies in seinem Referat auch auf neueste Sicherheitsrisiken durch mobile Devices hin. So haben Wissenschafter der City University of Hong Kong und der Indiana University Bloomington mit der sensory malware „Soundcomber“ein Proof-of-concept vorgestellt, welcher in der Lage ist, sensible Daten wie Kreditkarten- und PIN-Nummern aus tasten- oder sprach-basierten Interaktionen mit dem Menüsystem von Android-Phones auszulesen, indem der Trojaner nur wenige, heimliche, also unverdächtige Permissions für den Zugang zum Audio Sensor des Systems benötigt und dabei gezielte Profile zur Kontext-Erkennung verwendet.

Ein weiteres Sicherheitsrisiko stellen Smartphone Keylogger dar. An der University of California haben Forscher mit „TouchLogger“ eine Android App entwickelt, um die Beziehung zwischen Anschlagsvibrationen und den eingetippten Anschlägen zu demonstrieren. Dabei macht sich die App einen neuen Side Channel – „Motion“ (Bewegungssensoren wie Accelerometers und Gyroscopes) – auf Touchscreen Smartphones mit Soft Keyboards zu Nutze. „TouchLogger“ extrahiert Features aus den Orientierungsdaten. Da das Antippen verschiedener Positionen am Screen unterschiedliche Vibrationen herruft, können die Anschläge schlussgefolgert werden. Die Privacy Attacking-App hat in der Tat 70 % der getippten Anschläge auf einem Soft Keyboard mit ausschließlicher Nummerntastatur richtig rückgeschlossen. Die Forscher gehen davon aus, dass die Performance auf Tablet Computern und Devices mit größerem Screen sogar noch besser sein dürfte.

Der AIT-Sicherheitsexperte Thomas Bleier schloss seine Ausführungen zum Thema „Jugend im Cyberspace – Security als Schlüsselwort“ mit dem Appell, künftig in Sachen Sicherheit den richtigen Mittelweg zu gehen. Da davon ausgegangen werden kann, dass die heutigen Nutzer, die Jugendlichen, schon in Kürze auch Entwickler und Betreiber von neuen, innovativen IKT-Lösungen sein werden und auch in Entscheiderpositionen sitzen werden, empfiehlt er ihnen zwischen Bequemlichkeit, Funktionalität und Geschwindigkeit von Anwendungen auf der einen Seite und Sicherheit auf der anderen immer behutsam abzuwägen, als Cybersecurity-Fachmann wohl wissend, dass ein Mehr an Sicherheit, immer Abstriche bei der angestrebten Performance bedeutet.

3 Keynote „Cyberspace is our Space"

Gerfried STOCKER, Künstlerischer Leiter, Ars Electronica Linz

Gerfried Stocker, Künstlerischer Leiter der Ars Electronica Linz, kam bei seiner Keynote gleich zu Beginn sehr pointiert auf den Punkt. Facebook ist bevölkerungsmäßig das drittgrößte Land der Welt und wir sind alle Teil dieses großen Experiments, von dem wir noch nicht wissen wie es ausgehen wird. „Cyberspace is our space" und wir können diesen virtuellen Raum für uns nur dann sicher gestalten, wenn wir einen informierten und selbstbestimmten Umgang mit den neuen digitalen Kommunikationsmedien entwickeln. In Bezug auf Cyber Security haben die begeisterten Pioniere der neuen, digitalen Welt scheinbar einige Dinge übersehen, die wir jetzt in den Griff bekommen müssen.

Derzeit herrscht vor allem in der Elterngeneration, bei den so genannten „digital immigrants" einigermaßen Verunsicherung gegenüber den langsam alles vereinnahmenden sozialen Medien. Das ist aber kein Phänomen, welches sich erst zu Zeiten von Facebook oder Twitter auftat. Die Menschen hegten schon immer große Ängste gegenüber neuen Kommunikationsmedien – und zu Tode gefürchtet ist auch gestorben, so Stocker launisch.

Als Beispiel für historische Medienskepsis nannte er den optischen Telegraphen, den der französische Techniker Claude Chappe während der Wirren der französischen Revolution entwickelte. Mit dieser Telegrafie-Vorrichtung, auch Flügeltelegraf oder Semaphor genannt, konnte man mit Hilfe von schwenkbaren Signalarmen je nach Position anhand eines Codes 196 unterschiedliche Buchstaben zur nächsten Station signalisieren. 1794 überbrückte eine Telegrafenlinie die 270 Kilometer zwischen der Hauptstadt Paris und dem nördlich gelegenen Lille mit 22 Semaphorstationen. Die einzelnen Stationen standen je nach Sichtverhältnissen zwischen neun und zwölf Kilometer voneinander entfernt, so dass man mit einem Fernrohr die Zeichen der Nachbarstation einwandfrei erkennen konnte.

Bis 1845 entstand auf Basis dieser Technologie von Paris ausgehend ein flächendeckendes Telegrafennetz, welches die Hauptstadt mit allen wichtigen Städten Frankreichs verband. Noch heute kann ein Chappe-Telegrafenturm bei Saverne im Elsass gut erhalten besichtigt werden. Als skurril bezeichnete Stocker die damalige Furcht der Militärs, dass diese Kommunikationseinrichtungen von Unbefugten ausgespäht und so geheime Depeschen auch mitgelesen werden könnten. Das

führte erstens zur Einführung von Geheim-Codes und zweitens wurden die Telegrafenstationen von mehr Soldaten bewacht, als es Bedienstete für die Bedienung des Kommunikationssystems gab.

Die Überwachung und Bespitzelung von Kommunikation ist wohl untrennbar mit deren technischer Entwicklung verbunden, führte Stocker weiter aus. So wies z.B. Kaiser Joseph II im Jahr 1786 die Statthalter der österreichischen Erblande mit einer geheimen Instruktion an, den Betrieb von so genannten kleinen Posten und deren Briefkästen nur solchen Personen zu übertragen, von deren Rechtschaffenheit und Abhänglichkeit die Polizei versichert wäre. Postgeheimnis und Datensicherheit waren auch dem Chef des Pariser Rechnungshofes zweitrangig. 1759 warb er für die Vorteile der „petite poste" mit dem Argument, dass die Polizei mit der kleinen Post erstmals ein Mittel besäße, um die Adressen aller Leute zu ermitteln.

Und im 61. Kapitel von Alexandre Dumas „Der Graf von Monte Christo" (1845/1846) erlangte ein Telegraf traurige literarische Berühmtheit, indem er dazu genutzt wurde, mit einer gefälschten Botschaft einen Börsenbetrug durchzuführen. Zeitpunkt des Missbrauchs war das Jahr 1839, moderne, zeitgenössische Parallelen sind aber durchaus erkennbar.

Cybercrime ist heute in aller Munde. Nicht ganz ohne Berechtigung. Denn mit der Einführung neuer Kommunikationstechnologien, mit dem Schaffen einer neuen technologischen Realität hinkt die gesetzliche Realität zu Beginn immer hinterher. Daher kommt es auch anfänglich immer zu total überzogenen Reaktionen. Erst wenn die Gesetzsprechung mit einem entsprechenden Rechtsrahmen langsam nachzieht, beginnen sich auch die Wogen zu glätten. Für den Künstlerischen Leiter der Ars Electronica ist es in diesem Zusammenhang aber wichtig, bei der Regulierung von Kommunikationsmedien immer mit Augenmaß vorzugehen und auch eine ausgewogene Balance zwischen Sicherheits- und Freiheitsbedürfnis zu achten. Dies gelingt nur wenn sich die Gesellschaft intensiv mit der Thematik befasst.

Das gleiche gilt auch für die Erziehungssituation im Elternhaus. Eltern dürfen sich nicht entmutigen lassen und müssen gemeinsam mit ihren Kindern alle Möglichkeiten einer adäquaten Mediennutzung durchspielen und so ihren Nachwuchs mit den heute relevanten Kulturtechniken vertraut machen. Für Stocker ist hier die Gesprächsbasis zwischen Eltern und ihren Kindern das wichtigste. Diese stellt sich irgendwann automatisch ein, wenn wechselseitig auf bi-polare Aussagen gelassener regiert wird und führt dann in letzter Konsequenz zu jener Verantwortung, die wir im Umgang mit neuen Medien heute so dringend brauchen.

Die neuen Kommunikationsmedien stehen auch im Fokus von Medienkünstlern die mit ihren Produktionen uns alle zum Nachdenken anregen wollen.

So hat die österreichische, in London lebende Filmemacherin Manu Luksch 2007 mit einem „Science Fiction"-Märchen der besonderen Art für Aufsehen gesorgt. Die britische Hauptstadt verfügt über die höchste Dichte an CCTV-Kameras (Closed Circuit Television). Alleine in der Regierungszone Whitehall sind, rechtlich gedeckt durch SOCPA (Serious and Organized Crime and Police ACT), an die 300 CCTV-Kameras installiert.

Manu Luksch hat diesen Umstand einer nahezu omnipräsenten Überwachung Londons mit privaten Kameras dazu genutzt, ihr auf mehrere Jahre anberaumtes Projekt „Faceless" durchzuführen. Die Filmkünstlerin ließ sich an verschiedensten Orten der Londoner City von CCTV-Kameras filmen.

Dann fand sie heraus, dass ihr auf der Grundlage des „Data Protection Acts 1998" das Recht zustand, von den Betreibern der einzelnen Kamerasysteme die Herausgabe von Filmaufnahmen zu fordern, in denen sie bildlich erfasst wurde. Diesbezügliche Anfragen von Betroffenen müssen von den Betreibern laut Gesetz innerhalb von 40 Tagen bearbeitet werden, die dafür festgelegte Gebühr beträgt 10,- £ (Pound Sterling). Außerdem sind die Betreiber der Kamerasysteme aus Datenschutzgründen verpflichtet die Gesichter sämtlicher Personen auszuschwärzen, die in den Aufnahmen außer der anfragenden Person noch vorkommen. Im einem Fall von Kameraaufnahmen einer High Street Bank lieferte der Inhaber des Filmmaterials alle Bilder als gedruckte Stills (Hardcopies, Fotos von den einzelnen Filmframes), auf denen die Gesichter anderer Personen aus Identitätsschutzgründen mit Nagelscheren ausgeschnitten worden sind.

So kam Manu Luksch die Idee für ihren Filmtitel „Faceless" – gesichtslos. Mit hunderten von CCTV-Kameraaufnahmen, für die zwar die Locations für einzelne Szenen geplant wurden, entwickelte sie ein Drehbuch im nicht herkömmlichen Sinn, mit dem eine Utopie-lose Zukunft unserer Gesellschaft gezeichnet wurde, in der die Zeit zu existieren aufhört und die Welt sich im permanenten Zustand des Jetzt befindet.

In dem Artikel „Faceless: Chasing the Data Shadow" („Gesichtslos: Die Jagd nach dem Datenschatten") haben die Aktivitsten von „ambienttv.net", Manu Luksch und Makul Patel bei der Erklärung ihres Filmkonzeptes als „rechtliches Ready-made", also Bildern mit einem rechtlichen Überbau, eine Anleihe in der Literatur genommen:

Undeutliche Schreckgespenster einer Bedrohung, die über zeitkodierte Überwachungskameras festgehalten wurden, rechtfertigen ein umfassendes Netz voyeuristischer Kameralinsen. Ein Netz teilnahmsloser Beobachtungsgeräte, die jede Straße, jedes Gebäude abtasten, um die Möglichkeit einer Vergangenheit, die freie Wahl, etwas zu vergessen, auszuschalten. Glanzpunkte, besondere Augenblicke kann es

nicht mehr geben: Eine diskrete Tyrannei des „Jetzt" ist im Entstehen. „Realzeit" in ihrer pedantischsten Ausprägung.

Sinclair, Ian: *Lights out for the territory*, Granta, London 1998, S. 91

Manu Luksch und Makul Patel erklären Konzept und Titel ihres œuvre d'art noch etwas genauer: „Der Film spielt in einer geradezu unheimlich vertrauten Stadt, in der ein neu eingeführter Echtzeitkalender Vergangenheit und Zukunft abschafft, wodurch die Bürger von Schuld, Bedauern, und Zukunftsangst befreit sind. Ohne Gedächtnis oder Erwartung verblassten die Gesichtszüge und wurde die Bevölkerung sprichwörtlich gesichtslos. Eine Zeit unvorstellbaren Glücks beginnt – bis eine Frau ihr
Gesicht wiedererlangt …Tilda Swinton verlieh dem Plot ihre Erzählstimme

Der gesamte 50-minütige Film wurde nach den Richtlinien des „Manifesto for CCTV Filmmakers" gedreht, d.h. es wurde keine zusätzliche Kameraausrüstung außer den ohnehin in Betrieb befindlichen CCTV-Überwachungskameras verwendet. Da es vielfältige Schwierigkeiten bei der Anwendung der Bestimmungen des Data Protection Acts 1998 und Human Rights Acts von 1998 gab, die auch darin gipfelten, dass Kontrolleure der Kamerabilder von Existenz der gesetzlichen Grundlagen keine Ahnung hatten und daher Aufnahmen nicht immer erhältlich waren, musste die Geschichte on process ständig umgeschrieben werden.

„In Summe hinterfrägt der Film die Gesetze, die die Videoüberwachung der Gesellschaft regeln und die Kommunikationscodes, die ihre Umsetzung bestimmen, und ist sowohl durch seine Entstehungsweise als auch durch sein Plot eine Form der Kritik", so Manu Luksch und Makul Patel in dem o.a. Artikel.

Der Film „Faceless" ist fixer Bestandteil der „Collection Centre Pompidou" in Paris und wurde auf zahlreichen Filmfestivals, in Kunstgallerien, Museen, bei Menschenrechts-Events und in Jugendclubs gezeigt. Unter den vielen Shows und Screenings sind die nachfolgenden besonders erwähnenswert. Centre Pompidou (Hors Piste 2008), Galerie Motte et Rouet (Good Morning Paranoia, Paris 2008), Ars Electronica 2007, Diagonale 2007, dazibao, centre de photographies acutelles (FONCTION/FICTION 2008), Big Brother Awards und Quotidien sous contrôle von La Ligue des droits de l'Homme (Brüssel).

Noch alarmierender im Hinblick auf Cyber Security war das zweite Kunstprojekt, das Stocker am Summit präsentierte. Die beiden italienischen Medienkünstler Paolo Cirio und Alessandro Ludovico haben sich mit ihrer „The Hackining Monopolism Trilogy" drei Riesen des IT-Business – „Google, Amazon und Facebook"- als Zielscheiben ausgesucht, um Online-Sicherheitslücken aufzuzeigen. „Face to

Facebook“ bildete dabei den Schlusspunkt. Hier ging es Cirio und Ludovico darum, mit einer selbst generierten Software Facebook-Daten (Profilbilder, auf denen die meisten Benutzer lächeln, um möglichst viele Freunde im Netz zu finden, Namen, Länder aus denen die Nutzer kommen, Gruppen denen die Nutzer angehören, jeweils ein paar wenige Freundschaftsbeziehungen der Nutzer) von rund 1 Million Usern zu sichten und zu sammeln. Mit einer Datenbank wurden in Folge die lächelnden Gesichter analysiert. Nachdem die Datenbank fertig gestellt war, bauten die Medienkünstler einen Algorithmus, der auf selbstlernenden, neuronalen Netzen basierte, um die tausenden Bilder in sechs einfachen Kategorien („climber“, „easy going“, „funny“, „mild“, „sly“ und „smug“) gruppieren zu können. Die Software extrahierte dann mehr als 250.000 Gesichter.

Die beiden Italiener fanden auf Basis von wissenschaftlicher Literatur – Dan Jones „The Love Dilusion“ – und von durchgeführten Studien – Heather Rupp – heraus, dass Gesichter bei der Anbahnung von sexuellen Kontakten eine herausragende Rolle spielen. Nicht zufällig stehen sie daher auch im Zentrum des von Facebook aufgebauten sozialen Systems. Und obwohl Facebook keine Dating-Website im eigentlichen Sinne ist, baut es doch auf denselben Prinzipien auf. Daher war es für die Medienkünstler naheliegend, als letzten Schritt, die gesammelten und kategorisierten Daten aus ihrem Identitätsdiebstahl in einer Dating-Plattform neu zu kontextualisieren. Mit „Face to Facebook“ bekamen reale, von den Teilnehmern am größten sozialen Netzwerk der Welt selbst erstellte und hochgeladene Daten noch konkreter jene Nutzungsrichtung und Absicht, weswegen sie eigentlich schon für Facebook erstellt worden sind: nämlich neue, bislang unbekannte Leute zu finden, die man mit der virtuellen Präsenz anziehen kann.

Die Dating-Plattform der beiden Italiener hat das Vertrauen, welches Abermillionen Nutzer in Facebook gesetzt haben, arg in Zweifel gezogen. Mit „Face to Facebook“ wurde der Beweis erbracht, wie einfach persönliche Daten gestohlen und in einer neuen virtuellen Umgebung rekontextualisert werden können. Das Experiment hat auch demonstriert, wie fragil und potenziell manipulierbar die größte Online-Umgebung unserer Tage tatsächlich ist.

Natürlich hat es nicht lange gedauert, bis die Anwaltsmaschinerie von Facebook per gerichtlicher Verfügung die Schließung der Dating-Plattform durchsetzen konnte. In den Anschlussdiskussionen über das Experiment ging der Tenor der Meinungen bei Symposien und Kunstfestivals klar in die Richtung, dass dieses Unterfangen zwar legal fragwürdig war, weil private Daten ohne Wissen der Nutzer und des Plattform-Betreibers Facebook gesammelt, kategorisiert und in neuem Zusammenhang wieder veröffentlicht wurden, sich jedoch moralisch rechtfertigen ließ, weil die Verletzlichkeit von sozialen Online-Plattformen klar vor Augen geführt worden sind.

Datenmissbrauch erfordert immer eine gewisse Divergenz in der Betrachtung. Damit kam Stocker in seiner Keynote zum Schluss-Appell: „Wir müssen unsere Gesetze und Regulierungen auf eine veränderte Medienrealität anpassen!“

4 „Kinder und digitale Medien – Erwachsene, wo seid ihr?"

Carina FELZMANN, Geschäftsführung, Cox Orange Marketing & PR GmbH,
Sprecherin der Plattform „ARGE DigiKids"

Carina Felzmann begann ihre Präsentation mit einem Bonmot, welches kaum treffender die Ausgangslage des Umgangs von Kindern mit digitalen Medien beschreiben könnte: „How do you *THINK* my first day of kindergarten went?! They didn't even have Wi-Fi." Auch wenn es so dramatisch nicht sein mag, viel fehlt in der Realität der Digital Natives nicht auf diese Einschätzung. Kinder und Jugendliche haben sich jedenfalls schneller mit den neuen Möglichkeiten vertraut gemacht als Pädagogen und Eltern", so Felzmann.

Danach stellte Felzmann die Aktions-Plattform ARGE DigiKids vor, die auf eine Initiative von Cox Orange und dem Verein art:business zurück geht. Das Spektrum der Aktionen der Plattform reicht von der Beauftragung und Erstellung von Studien, über die Abhaltung von Konferenzen bis zur Durchführung von Webaktivitäten. Experten, Ministerien, das AIT (Austrian Institute of Technology GmbH), die RTR (Rundfunk & Telekom Regulierungs-GbmH), die OCG (Österreichische Computer Gesellschaft) und Unternehmen der Privatwirtschaft unterstützten die Arbeit dieser Aktions-Plattform.

Im Jahr 2011 wollte es das „Trio" Cox Orange, der Verein art & business Kulturmanagement und die Medienpädagogin Dr. Geretschläger genau wissen, wie Kinder und Jugendliche heute in Österreich ihren digitalen Alltag erleben und wie die Unterstützung durch Eltern und Lehrkräfte erfolgt, bei dem was sie online machen. Eine Studie sollte darauf Antworten geben. Die qualitative Marktforschungsstudie „Digikids 2011" war vom Design her einmal anders konzipiert. Um den digitalen Alltag von 10 bis 15-Jährigen zu simulieren, organisierte die Agentur PGM mit 63 „Digikids" einen Open Space bzw. ein World Café. Dabei luden sechs Themeninseln, unterstützt von jugendlichen ModeratorInnen, zur gemeinsamen Auseinandersetzung über soziale Netzwerke, Surfen und Spielen im Internet, Internet in der Schule, Sicherheit im Netz, die Vorbildfunktion von Role Models, Eltern und Lehrkräften.

Die Ergebnisse kann man so kurz auf einen Nenner bringen: Österreichs Kinder und Jugendliche sind technisch bestens ausgestattet, ständig digital verbunden

und das ab dem 8. Lebensjahr. Das Einstiegstool ist das Handy, was im Handyland Österreich nicht verwundert. 100 % der TeilnehmerInnen an der Studie hatten ein Handy, jedes zweite davon war auch Internet tauglich. Für jene 38, die über keinen eigenen Laptop verfügen, stellt das Handy den Basiszugang zum Internet dar.

In Österreich nutzen 53 % das Web über das Handy, während es in Europa auf Basis der aktuellen „EU Kids online"-Studie mit 25.142 Digikids zwischen 9 und 16 Jahren nur an die 34 % sind.

Für die 10 bis 12-Jährigen steht Spielen im Internet im Vordergrund. Mit zunehmendem Lebensalter der Kinder wird die Kommunikation über soziale Netzwerke umso bedeutender. Bei den Jugendlichen dominieren wenige Websites, diese werden dafür aber im Sinne der Verlagerung von analogen Aktivitäten ins Netz umso intensiver genutzt. Es konnten auch Gender-Unterschiede festgestellt werden: Bei Buben genießen Fußballseiten wie z.B. „laola1" regen Zuspruch, Mädchen fokusssieren eher auf Girlie-Seiten zu Trend- und Lifestyle-Themen. Die Inklusion sozialer Gruppen ist weit fortgeschritten. Im Hinblick auf Nutzungsintensität sind keine nennenswerten Unterschiede zwischen Kindern mit und ohne Migrationshintergrund erkennbar, eher sind es sprachlich oder kulturell dominierte Präferenzen.

Weiters ergab die Studie, dass die Heranführung an digitales Know-how in erster Linie durch die Familie erfolgt. In Bezug auf Role Models und Vorbilder stellten die SchülerInnen einen technischen Gender-Gap, also Unterschiede hinsichtlich der technischen Kompetenz zwischen Vätern und Müttern fest. Väter kennen sich besser aus und die Eltern sind generell versierter als LehrerInnen.

Facebook ist bei den Digikids ein wirklicher Renner. 65 % der an der Studie beteiligten Jugendlichen nutzen Facebook und 57 % haben ein eigenes Profil. Mehr als die Hälft chattet über Facebook mit Freunden aus dem nahen sozialen Umfeld, 32 % suchen gezielt Freunde, 29 % spielen Games und 25 % nutzen Facebook um in Kontakt zu bleiben oder News auszutauschen.

In der Kommunikation mit Gleichaltrigen haben E-mails so gut wie keine Bedeutung. Die primäre Kommunikation erfolgt mit 50 % über das Handy, 30 % verschicken SMS und 35 % nutzen Facebook.

Die an der Studie beteiligten SchülerInnen haben ein hohes allgemeines Problembewusstsein. 53 % jener, die in Facebook ein Profil angelegt haben, gaben an, schon belästigt worden zu sein. Auf der anderen Seite wiegen sich die Kinder in Facebook aber auch in einer Art Scheinanonymität, in man sich „virtuell" zeigt, ohne sich viel

Gedanken zu machen. Die Kids fühlen sich auch deswegen im Netz sicher, weil es das Medium erleichtert, Grenzen zu überschreiten.

Die PGM-Studie förderte auch zu Tage, dass die Eltern aus Sicht der Kinder keine echten Sparring-Partner sind, die Kids sich aber durchaus Hilfe und Support in ihrer Sprache wünschen würden. Gemeint sind hier z.B. Anleitungen bei Recherchen und bei der Bewertung von Inhalten und Informationen über Schutz und Sicherheit im Netz. Die meisten Eltern sind jedoch auf Grund des Nachteils der geringeren Technologiekenntnis verunsichert. Auch sehen sie noch zu sehr nur Gefahren in der realen Welt. Daher können sie dem Nachwuchs bei Problemen und Sorgen im Netz keine kompetente Unterstützung bieten. Kinder und Jugendliche sind zwar versierte Technologie- und Medienanwender, sie benötigen aber künftig verstärkt die Vermittlung von Medienkompetenz und sozialer Kompetenz.

Die DigiKids 2012 Studie lieferte als Conclusio dann einen Forderungskatalog der jungen Generation an Eltern, Lehrer und die Politik.

Von den Eltern wünschen sich die Kinder, dass der Freiraum im größten ungeregelten Raum erhalten wird, ihre Aktivitäten im Netz begleitet und angeleitet werden, die soziale Kompetenz der Kinder hin zur Eigenverantwortlichkeit gestärkt wird und dass die Eltern selbst computer- und internetfit werden, um mitreden zu können.

„Wir brauchen ein stärkeres gesellschaftliches Bewusstsein für die Herausforderung unserer Zeit. Eltern- und Schulbildung sind notwendig", mahnte Frau Univ.-Prof. Dr. Ingrid Paus-Hasebrink, Dekanin der Kultur- und Gesellschaftswissenschaftlichen Fakultät der Universität Wien, im Rahmen des Digikids-Kongresses 2011 ein.

Von ihrer LehrerInnen verlangen die DigiKids mehr Offenheit für ihre Aktivitäten im Netz und ein stärkeres Interesse an neuen Medien. Die Schule sollte Internet & Co als Arbeitsmedien ergänzend zu übrigen Ressourcen im Unterricht anbieten und Schulplattformen zum sozialen und inhaltlichen Austausch für Übungs- und Lernzwecke anbieten. Für die Kinder und Jugendlichen wären Hausübungs-, Schularbeits- und Maturabeispiele zum Download wünschenswert.

„Es ist wichtig, dass die Schule die technische Entwicklung aufgreift und Schülern und Schülerinnen die digitalen Kompetenzen vermittelt, die sie für ihr zukünftiges Lenben brauchen" stellt sich Mag. Heidrun Strohmeyer, bm:ukk, Leiterin des Bereichs Informationstechnologie voll auf die Seite des Nachwuchses beim 2011er-Kongress.

Von der Politik selbst fordern die Jugendlichen Angebote zur Auseinandersetzung mit Politik im Internet sowie Datensicherheit und technische Möglichkeiten zum Schutz der Privatsphäre.

Prof. Dr. Bernd Schorb, vom Institut für Medienpädagogik und Weiterbildung zog als gewichtiges Sprachrohr im Rahmen des Digikids-Kogresses im Sinne der Jugendlichen einen plakativen Vergleich: „Staaten wurden gegründet, um BürgerInnen vor Partikularinteressen zu schützen. Im Web gibt es wirtschaftliche Partikularinteressen. Daher sollten Jugendliche vom Staat verlangen, geschützt zu werden."

Die im April 2012 präsentierte DigiKids neue Studie bildete den Ausgangpunkt für die vom 4.-5. Mai 2012 veranstaltete „verkehrte Konferenz – Kinder und digitale Medien". Im Vorfeld der Konferenz fanden Workshops mit Jugendlichen aus verschiedenen Altersgruppen und mit unterschiedlichem sozialen Background statt. Diskutiert wurden die Fragen, was erwarte ich mir zum Thema Digitale Medien von Eltern, Lehrkräften und Politiker/innen. In Folge trafen sich die Jugendlichen mit Entscheidungsträgern aus der Politik zur Diskussion. Durch Einbeziehung von Jugendlichen aus ländlichen Gebieten und von Jugendlichen mit Migrationshintergrund, sollten auch die Forderungen und Wünsche dieser Jugendgruppen Berücksichtigung finden.

Aus diesen Workshops ergab sich folgendes großes Bild:

- Das Positive des www in den Mittelpunkt stellen
- Internet weiterhin als freien Raum erleben können
- Prävention anstatt Überwachung und Restriktion
- Begleitung zur Eigenverantwortung und Einschätzung der Risiken
- Datensicherheit und technische Möglichkeiten zum Schutz der Privatsphäre ausbauen
- Medienkompetenz der Erwachsenen stärken
- Altersgerechte Angebote zur Auseinandersetzung mit Politik im Internet

Die Ergebnisse wurden in Folge auch bei der „Verkehrten Konferenz" präsentiert, wo es darum ging, dass beide Seiten, die Erwachsenen und Jugendlichen voneinander lernen. Beide Gruppen über unterschiedliche Kompetenzen in der digitalen Welt, der Austausch fand bei der Verkehrten Konferenz zur Begeisterung aller Beteiligten statt.

Zwei Schulen wurden zu Projektpartnern: die Polytechnische Schule PTS 18, Pyrkergasse und das Goethegymnasium in der Astgasse. Sie hatten die Aufgabe, bei der Konferenz einen Teil Moderation zu übernehmen, den Erwachsenen zu erklären, wie ihr digitaler Alltag aussieht und die Interviews mit Vertretern von

Institutionen zu führen. Die SchülerInnen erhielten zur Vorbereitung verschiedene Coachings. Zum einen Mentaltraining des Institutes Kutschera, um im richtigen Moment emotional mit Freude gut zu „performen", zum anderen Regieanweisungen von Geraldine Kilgus, ihres Zeichens Lehrbeauftragte für Theater an der Montessori Schule Mödling und Clinicclown.

Am ersten Konferenztag erhielten die 10- bis 14-Jährigen an Thementischen Informationen über Facebook, Recht am eigenen Bild, Liebe im Netz, Online-Reputation, Handys und Apps, Online shopping sowie Bilder und Musik richtig nutzen. Auf die 14- bis 18-Jährigen warteten Vorträge über Social Media, Cybercrime oder die effiziente Internetrecherche ergänzten das Programm für die Unterstufenschüler/innen.

Am zweiten Konferenztag hatten dann die Oberstufen-SchülerInnen ihren Bühnenauftritt und erklärten den Erwachsenen von ihren Erfahrungen mit Web 2.0, mit Online-Spielen und Handyapplikationen. In Folge wurden die Erwachsenen zu den Thementischen eingeladen, um über Facebook, Handy und Computerspielen die „digital natives" direkt befragen zu können und so als „digital immigrants"dazulernen .

Cox Orange konnte für das Projekt die Pädagogische Hochschule Wien und Saferinternet.at gewinnen. Saferinternet schulte an die 30 StudentInnen der PH Wien auf das Webthema ein, die StudentInnen betrreuten am ersten Konferenztag die Thementische der Unterstufe und unterstützten die SchülerInnen am zweiten Konferenztag bei ihren Präsentationen.

Veranstalterin, C. Felzmann: „Ich war sehr beeindruckt, wie kompetent die Jugendlichen bei der ‚verkehrten Konferenz' aufgetreten sind! Sie haben ihre Fachkenntnisse perfekt präsentiert und moderiert. Unser Ziel, Generationen zu vernetzen und voneinander zu lernen haben wir in diesen zwei Tagen sicher erreicht."

Zum Abschluss ihrer Präsentation gab Carina Felzmann, mit Daten aus dem Jugend-Trend-Monitor 2012 einen kurzen Ausblick auf DigiKids 2013.

Auf die Frage „Welchen **Stellenwert** haben folgende Bereiche in deinem Leben?" haben 67 % der Jugendlichen (männlich: 57,5 %, weiblich: 76,9 %) **für Familie gevotet**.
Auf Platz 2 folgen Freunde mit 66% (männlich: 61,7 %, weiblich: 71,8 %).
Auffallend ist hier, die **Wichtigkeit von Freunden** in der Gruppe 14-19 Jahre mit 75,1 % am höchsten ist. Mit zunehmendem Lebensalter fällt diese Quote (20-24 Jahre: 68,4 %, 25-29 Jahre: 54,1 %). An die dritte Stelle im Ranking schaffte es **Gesundheit** mit 56,2 % (männlich: 49,9 %, weiblich: 62,9 %).

Auf die Frage „Welche Werte sind dir persönlich am wichtigsten?“ antworteten 62,8 % mit **Ehrlichkeit**/Offenheit/Aufrichtigkeit, was Platz 1 bedeutete.
Die Familie folgte mit 62,5 % auf Platz 2 und Rang 3 ging an Verlässlichkeit.

Für 2013 gab Carina Felzmann drei große DigiKids Ziele aus: Marktforschung, Abhaltung eines zweitägigen Kongresses zum Thema „Arbeitswelt, wir kommen! und Teilnahme an den Alpbacher Technologiegesprächen mit „Erfahrungen & Werte“.

5 „ÖAMTC young & mobile – Social Media als Kommunikationsform eines traditionellen Clubs mit seinen Jugendmitgliedern"

Paul HAIMOVICI, Jugendmarketing, ÖAMTC
Harald GRABNER, Gründer und Geschäftsführer
123CONSULTING e.U.

Paul Haimovici, Verantwortlicher für das Jugendmarketing beim ÖAMTC, begann seine Präsentation mit ein paar allgemeinen Infos zum Club. Die Mission des ÖAMTC ist die „Sicherstellung und Förderung der individuellen Mobilität in einer lebenswerten Umwelt. Dabei baut der Club auf folgende Grundsätze: Föderaler Aufbau (7 Landesvereine), Überparteilichkeit, wirtschaftliche Unabhängigkeit und Internationale Verankerung. Der ÖAMTC unterhält mit dem Versicherungs-Service, dem Reisebüro, dem Verlag (Clubmagazin auto touring), dem Clubartikelhandel (Shops) und der Fahrtechnik fünf Tochtergesellschaften.

Der Club kann auf eine positive Entwicklung bei den Mitgliedschaften verweisen. Gab es im Jahr 2005 schon 1.558.199 Mitglieder, waren es 2010 bereits 1.785.151 Mitglieder und im Jahr 2012 stieg die Zahl auf 1.884.134. Die Altersstrukturen der ÖAMTC Mitglieder korrespondieren in etwa mit der gesellschaftlichen Altersstruktur Österreichs. Beim ÖAMTC gibt es unterschiedliche Mitgliedsarten wie Auto (€ 75,50), Motorrad (€ 42,10), Touring (€ 16,90) und Firmenmitgliedschaft (€ 75,70, jedes weitere Firmenfahrzeug € 42,10).

Auch bei den Jugend-Mitgliedschaften bietet der Club mehrere Möglichkeiten: Gratis-Mitgliedschaft für Kinder (0-14 Jahre) und Jugendliche (15-19 Jahre), ermäßigte Mitgliedschaft für junge Erwachsene (20-23 Jahre) und eine Gratis-Schnupper-Mitgliedschaft (für Führerschein-Neulinge, Grundwehr- und Zivildiener).

Mit der Gratis-Mitgliedschaft kommen junge Mitglieder in den Genuss zahlreicher Vorteile wie z.B. Führerschein-Infos von A-Z, Gratis Touring-Set & Reiseservice, alle Informationen zum Autokauf, Pannenhilfe von 0-24 Uhr, Preisvorteile mit der Clubkarte und einer Gratis Privat-Haftpflicht- und Unfall-Versicherung.

Danach berichtet Haimovici über Vorgangsweise der Strategie von young&mobile: „Zuerst haben wir Basis-Infos besorgt. Die Daten kamen aus Focus Gruppen, Jugendstudien, von Trendscouts (T-factory JourFix), vom monatlichen Goldbach

Media Trendreport, von den IAA-News (International Advertising Association), aber auch direkt von Jugendreise- und Eventveranstaltern sowie Szenelokal-Betreibern. Ergänzend wurden verschiedenste Studien wie Gfk Social Networks, Gfk Jugend Online, AGTT/Gfk Fernsehforschung, JIM Studie, Marketagent Studie etc. herangezogen und ausgewertet".

Im Jahr 2010 hat der ÖAMTC dann einen Relaunch durchgeführt und das Design auf die Zielgruppe young&mobile optimiert. Mit dieser grafischen Neuausrichtung wurden auch die Inhalte und die Sprache angepasst. Mit stärkerer Kommunikation und Darstellung positiver Aspekte, mit gut lesbaren und verständlichen Textelementen und der Ansprache mit „Du" fand der ÖAMTC den richtigen Stil für die Interaktion mit seinen jugendlichen Mitgliedern. Der Club fungiert für diese Zielgruppe als „Mobilitätsenabler", so Haimovici.

Das innovative Neukonzept „Neues Design – Neue Medien – Neue Ansprache" bildete dann das Fundament für den Online-Auftritt von ÖAMTC young&mobile. Durch die digitale Vernetzung ist der Club dort, wo sich die User befinden. Die ÖAMTC young&mobile Website (www.oeamtc.at/young) überzeugt mit einfacher Navigation und übersichtlicher Darstellung der jugendrelevanten Inhalte. Der Newsletter wurde der neuen Linie angepasst und wird jeweils am letzten Freitag im Monat verschickt. Zusätzlich zur mobilen Website ist der Club mit den ÖAMTC Apps, wie z.B. dem Führerschein-Quiz und dem City Guide, auf allen mobilen Devices wie Smartphones und Tablets vertreten. Der Community Aufbau erfolgte über die sozialen Netzwerke Facebook, Google plus und YouTube.

Die neue Website überzeugt mit klarer Navigation und liefert Inhalte aus den Bereichen Führerschein, Auto&2-Rad, Reisen, On The Road sowie Fun&More. Oberste Ziele auf der Website sind die Zusammenfassung von jugendrelevanten Themen, zielgruppengerechte Aufbereitung der Inhalte und regelmäßige Aktualisierung.

Der Newsletter wird jeweils am letzten Freitag im Monat versandt. Im inhaltlichen Aufbau enthält er 1 Hauptthema, mehrere Nebenthemen und den Newsticker „TIPP". Das Design des young&moible Newsletter entspricht der Jugendlinie des ÖAMTC. Dieses Kommunikations-Tool erweist sich mit den höchsten Öffnungs- und Klickraten innerhalb des Clubs als äußerst effizient.

Im April 2012 hat ÖAMTC young&mobile eine Social Media Umfrage durchgeführt. Die Datenerhebung erfolgte in Form einer Online-Umfrage mittels Mailversand. Die Ziele dieser Marktforschung waren die Analyse der einzelnen ÖAMTC Facebook Seiten, die Messung der Zufriedenheit und die Einbindung von Ideen und Wünschen. Dabei wurden Fans und „nicht" Fans befragt.

Haimovici zu den wichtigsten Ergebnissen: „Mehr als 66% der 15-24 Jährigen ÖAMTC Fans nutzen Facebook mehrmals täglich, 18% zumindest einmal täglich. Bei der Frage nach den Motiven für das Fan-Sein gaben 73% an, dass sie an Infos über Aktivitäten des ÖAMTC interessiert sind, 44% möchten ihre Unterstützung gegenüber dem Club zeigen, 43% möchten über Neuigkeiten informiert werden und 35% dieser Zielgruppe nehmen gerne an Gewinnspielen teil".

68% der young&mobile Fans bewerten den Facebook Auftritt als sehr gut, 29% als gut. 54% aller Fans lesen regelmäßig die Postings, 54% der Fans finden die redaktionellen Themen sehr gut und 41% gut. Beim Post Wording vergaben 44% der Fans ein sehr gut und 40% ein gut. Auch in Punkto Post-Häufigkeit wird dem Facebook Auftritt von ÖAMTC young&mobile ein gutes Zeugnis ausgestellt: 87% sind sehr zufrieden. „Das sind herausragende Ergebnisse", so Haimovici, „die unsere geplante Social Media Strategie in hohem Maße bestätigt hat."

ÖAMTC young&mobile, das Jugendsegment des Österreichischen Automobil-, Motorrad- und Touring Clubs, wird von 123Consulting, der Wiener Agentur für Social Media & Online Marketing, beraten. Daher übernahm beim Cyber Security Summit auch Harald Grabner den weiteren Vortrag, um den Tagungsteilnehmern die Strategie, Entwicklung und Optimierung des Facebook-Auftritts und die Entwicklung von Spiele-Applikationen für ÖAMTC young&mobile näher zu bringen.

Das Design der Facebook Site von ÖAMTC young&mobile wurde den anderen Online Medien angepasst. Die Besucher der Facebook Site können sich mit einem Klick in Gewinnspiele einloggen, Informationen zu Führerschein, Reisen, Auto & 2-Rad abrufen, sich für den Newsletter anmelden und die Gratis-Mitgliedschaft für alle zwischen 15 und 19 Jahre beantragen. Der gepostete Content verweist in erster Linie auf die Website, um die Jugendlichen mit weiteren Informationen zu den einzelnen Themen zu versorgen.

ÖAMTC young&mobile hatte sich zum Ziel gesetzt, bis zum Jahresende 2012 10.000 Fans auf Facebook zu erreichen, das bereits im August übertroffen wurde. Die Zielgruppe der ÖAMTC young&mobile Facebook Site ist männlich (62%) und zwischen 13 und 17 Jahre alt. Bei der Herkunft dominiert Österreich mit 10.524 Fans, gefolgt von 939 Fans aus Deutschland, 171 aus den Vereinigten Staaten, 34 aus Ungarn, 32 aus Serbien. Einige Fans kommen aus der Schweiz, Spanien, Italien, Großbritannien und Frankreich. Somit stößt die Facebook Seite auch auf internationales Interesse.

Die Seite erzielt im Schnitt 886.200 Impressions und 24.500 Clicks pro Monat. Über 4.000 Fans sind regelmäßig echte Storyteller und interagieren mit Likes,

Shares oder Kommentaren. Die Zahl der „viralen Impressionen“ – User die mit der Seite interagieren – beträgt im Schnitt 137.100.

Der redaktionelle Mix auf Facebook spiegelt Themen aus Information, Service und Unterhaltung wieder. Angereichert mit top-aktuellen Themen, Experten-Tipps, Touristik Informationen, Führerschein Quiz und Grüße aus Schilda.

Für die Facebook Site wurden im Vorfeld von 123Consulting gemeinsam mit dem ÖAMTC Redaktions-Guidelines erarbeitet, die auch Richtlinien zum Kritik-Management beinhalten. Für den Facebook-Auftritt ist außerdem ein 24/7-Service eingerichtet, inklusive Redaktion- , Anfrage und Kritikmanagement.

Danach präsentierte Harald Grabner ein kleines „Best-of“ von Facebook-Postings mit hoher Interaktionsrate. Darunter zum Beispiel: „Gewinne einen Bladerunner“ durch Klick auf die Gewinnspiel Zone, witzige Fotos mit entsprechender Betitelung wie „Blitzmarathon“ (Geschwindigkeitsmessung mit mobiler Radarpistole in Richtung einer auf dem Gehsteig mit einer Gehilfe ausgestatteten spazierenden Oma), Lustige Verkehrsschilder „Ausgenommen Raumfahrzeuge“ (Immer mehr Außerirdische lieben das Schwimmbad in Grein an der Donau), sowie Postings zum Führerscheintest und zum L17 Führerschein.

Bei der Entwicklung von jugendaffinen Facebook Spielen stand die Nachhaltigkeit und das spielerische Lernen der ÖAMTC Leistungen im Mittelpunkt. Zwei sehr erfolgreiche Beispiele der jüngsten Vergangenheit waren die Facebook Games „ÖAMTC City Stickers Reloaded“ und „ÖAMTC Trophy Austria“.

Bei erstem Gewinnspiel handelt es sich um ein virtuelles Sticker-Album im Netz, das knapp vor Beginn der Sommerreisezeit 2012 auf der Facebook-Site von ÖAMTC young&mobile implementiert wurde. Dabei konnten die Gewinnspiel-teilnehmer sich eine der zehn schönsten Städte Europas (Reiseziele des ÖAMTC City Guides: Amsterdam, Barcelona, Berlin, Brüssel, Lissabon, London, Paris, Prag, Rom, Zürich) auswählen und danach mit der Maus den passenden Sticker in das richtige Feld der Albumseite ziehen. Zu jeder Stadt gab es auch einen Infosticker mit ÖAMTC Touring-Set. Fertig „eingeklebte“ Fotos konnte man für eine Großan-sicht anklicken. Für jede Stadt gab es zwei Album-Seiten, doppelte Sticker waren grau unterlegt. Nachschub an Stickern bekam man durch Interaktion. User konnten einander neue Stickerpacks schenken und doppelte Sticker konnten mit anderen Usern getauscht werden. Wer mindestens ein Album vervollständigt hatte, nahm an einer Verlosung von Städtetrips, Zugtickets oder anderen Reisepreisen teil.

Die Idee hinter diesem Spiel war, die Kindheitserinnerungen an die beliebten Panini-Alben möglichst gefühlsecht in den digitalen Raum zu übertragen. Der

Erfolg war durchschlagend. Innerhalb der ersten zwei Tage waren die ersten 1.000 User aktiv. Insgesamt wurden im Gewinnspielzeitraum 873.309 Sticker gespielt und 302.781 Stickerpacks verschenkt.

Bei der ÖAMTC „Trophy Austria" wurden Kilometerkarten aufgedeckt und die Spieler fuhren damit virtuell alle Stützpunkte des ÖAMTC an. Wer eine Pannenkarte aufdeckte blieb so lange am gleichen Fleck stehen, bis ihm ein Freund ein ÖAMTC Pannenfahrzeug schickte. Alle 200 km erreichten die Spieler einen Stützpunkt und erhielten einen Pokal. Je mehr Pokale ein Spieler gesammelt hat, desto höher wurden seine Chancen auf einen der vielen Preise. Auch bei diesem Gewinnspiel konnte man an Freunde Karten verschenken oder Freunde um Karten bitten. Als Hauptpreis für dieses Facebook Game war unter anderem die Teilnahme an einem Kart-Rennen.

Zum Abschluss des ÖAMTC young&mobile Vortrags referierte Harald Grabner von 123Consulting noch über Gefahren und Sicherheit im Netz.

Aktuelle Zahlen belegen, dass bereits 11- bis 16-Jährige diversen Bedrohungen im Netz begegnet sind. 78% hatten schon einmal einen Virus auf ihrem Computer, 37% wurden mit Personen konfrontiert, die unter falschem Namen agiert haben. 22% der meist weiblichen Zielgruppe hatten schon negative Erfahrungen mit sexueller Anmache, 20% waren schon Beleidigungen im Web ausgesetzt.

In Summe kann ein bewussterer Zugang und zunehmende Sensibilisierung mit dem Web diagnostiziert werden. 85% teilen z.B. ihr Facebook Profil nur mit den eigenen Facebook Freunden, davon schalten 80% ihre Facebook Fotos nur für Freunde frei.

Beim Schutz vor Datenmissbrauch ist die jüngere Generation der 18- bis 24-Jährigen etwas weniger vorsorglich orientiert als die 55- bis 65-Jährigen. Bei der jungen Generation speichern nur 65,1% keine vertraulichen Daten, in der Gruppe der älteren Nutzer sind es 76,7%. Auch im Hinblick auf die Angabe möglichst weniger privater Daten sind die Jungen unvorsichtiger. Nur 52,3% sehen dies als Gefahr, während die 55- bis 65-Jährigen hier mit 73,3% weit stärker besorgt sind. Bei der Speicherung von Fotos wird die unterschiedliche Einschätzung noch gravierender. Nur 30,8% der 18- bis 24-Jährigen sieht im Speichern privater Fotos eine Netzgefahr während dies in der Gegenzielgruppe 58,5% sind. Online-Gewinnspiele sehen hingegen 47,1% der Jugendlichen als Gefahr während diese Einschätzung nur 40,9% der älteren Erwachsenen teilt. Das Achtgeben auf Datenverschlüsselung beherzigen 30,8% der 18- bis 24-Jährigen, bei den 55- bis 65-Jährigen macht der Prozentsatz hingegen 52,2% aus.

Allerdings sieht Grabner ein nicht zu unterschätzendes Gefahrenbewusstsein. Denn die jungen User zwischen 18 und 24 Jahren würden es den Tätern leicht machen.

Auf verschlüsselte Übertragung achte nicht einmal ein Drittel der Jugendlichen. In sozialen Netzwerken hingegen seien Jugendliche erfahrener und vorsichtiger als die „Fax-Generation". In Zukunft sei aber mit steigendem Gefahrenpotenzial zu rechnen, da die Methoden der Angreifer immer raffinierter und professioneller werden. Daher gewinne der Schutz persönlicher Daten und der persönlichen Identität weiter an Bedeutung.

In Sachen Sicherheit hält sich ÖAMTC young&mobile an die strengen nationalen und internationalen Datenschutz-Richtlinien und sorgt somit für Vertrauen auch im Netz. Die Nutzer erhalten immer verlässliche Auskunft über die Nutzung von Daten im Web und in den sozialen Netzwerken. Und mit der geplanten Implementierung einer eigenen Subsite zum Thema „Sicherheit im Web" mit weiterführenden Links stellt die Jugendsparte des Clubs allen Sicherheits-Interessierten die erforderlichen Informationen zum bestmöglichen Schutz im digitalen Leben bereit. Der ÖAMTC fördert zusätzlich mit Studien und gezielter Öffentlichkeitsarbeit sowie Informationen in den sozialen Netzwerken die Sensibilisierung und Aufklärung dieses Themas.

ÖAMTC young&mobile betreibt darüber hinaus kein Daten-Matching von fremden Quellen wie z.B. Facebook und schützt somit die Privatsphäre seiner User.

6 „The Identity Shift – Do you know what your children are doing?"

Revital MAROM, Head of Marketing & Consumer Insight, Alcatel Lucent

Revital Marom, bei Alcatel Lucent verantwortlich für Marketing und Konsumentenforschung (Consumer Insight), erklärte am Beginn ihres Vortrages beim „Cyber Security Summit" den Zusammenhang zwischen Technologie und Kultur bzw. gelernten Kulturtechniken. Technologie hat nach ihrer Ansicht immer eine Auswirkung auf aktuelle Lebenspraktiken und gesellschaftliche Alltagskulturen. Technologien und insbesondere Medientechnologien beeinflussen im weiteren Sinne auch die „angeborenen" Verhaltensweisen von ganzen Generationen. Marom nahm in ihrer Themeneinführung Anleihen bei den Erkenntnissen ihrer Alcatel-Kollegin Allison M. Cerra, die in dem Buch „Identity Shift: Where Identity Meets Technology in the Networked-Community Age" anhand von 5.000 Konsumenten in den USA untersuchte, wie Technologien und Lebenskulturen bei drei unterschiedlichen Generationen miteinander verwoben waren und wie sich der Gebrauch von Medientechnologien im Verlauf der einzelnen Lebensphasen (Adoleszenz, Elternschaft und Lebensmitte) auf die konkrete Ausformung von Lebenskulturen auswirkte.

So spielte z.B. das Fernsehen im Leben der „Boomer" eine zentrale Rolle bei der Gestaltung und Prägung der Jugendjahre während für die „Gen Xer" Spielekonsolen und der Joystick diese Funktion innehatten. Unsere heutige „Millennial"-Generation hingegen ist gekennzeichnet durch den ersten und frühen Gebrauch von Mobiltelefonen, mit denen sich die Angehörigen dieser Zeitgenossenschaft ihren unmittelbaren Status in Freundeskreisen erwarben. Durch diese Verschränkung von Technologie und Kultur wird auch erklärbar, warum sich bestimmte Generationen mehrheitlich dieselben Interessensperspektiven teilen.

Äußerst aufschlussreich für die eigentliche Themenstellung ihres Vortrages war dann die Vorstellung des Identitätskonzeptes, mit dem die zuvor angesprochene Studie von Alcatel Lucent qualitativ operierte. Identität setzt sich aus Presentation (Präsentation, Selbst-Image), aus Protection (Schutz persönlicher Daten, Privatsphäre etc.) und Preference (Präferenzen, Vorlieben) zusammen. Allison Cerra spricht in diesem Zusammenhang von „The 3 Ps of Identity".

Im Hinblick auf das selbst reflektierte Image, das Selbstbildnis, war die Welt im Vorstadion der Always-on Medien etwas einfacher. So konnte eine Person zwar

verschiedene Rollen einnehmen und mit ihnen zusammenhängend unterschiedliche Formen der Selbstdarstellung ausüben – z.B. zu Hause, in der Arbeit, bei sozialen Zusammentreffen im Freundeskreis, in der Kirche etc. – aber die Menschen hatten zumindest noch die Eigenkontrolle darüber, welches Image sie sich in welchem Situations-Kontext geben wollen. Die heutige Netzwerk-Gemeinschaft hingegen verlangt von jedem von uns eine allgegenwärtige und laufende Reflexion darüber, wer wir sind. Und bei ständig mit dem Netz verbundenen Kommunikationsgeräten haben Leute mit Anschluss an das Netz und mit einer bestimmten Meinung auch jederzeit die Möglichkeit, die Rollen von anderen zu unterminieren und zu kontrastieren, auch ohne Zustimmung der Betroffenen, indem sie z.B. einen für die gesamte Community sichtbaren Kommentar verfassen oder ein unerwünschtes Foto in den virtuellen Raum hochladen.

Das zweite P, Protection (Schutz der persönlichen Daten), wird durch die Ansicht von den Benutzern getrieben, indem sie selbst auswählen, was sie von sich preisgeben bzw. was sie über sich und ihre liebsten Angehörigen (Familie, Freunde) verschleiern wollen. Mediengeschichten mit Sicherheit als Aufhänger zählen zu den Rennern der öffentlichen Kommunikation, weil scheinbar die Gesellschaft fasziniert darüber ist, wie verletzlich die virtuelle Welt, die uns umgibt letztlich sein kann. Aber nicht alle Sicherheitsattacken haben die gleich schweren Konsequenzen. So macht es z.B. einen Unterschied, ob jemand mit ärgerlichen Spam-Mails belästigt wird, oder ob jemand durch Identitätsklau (Diebstahl von Identitätsdaten) in seinem gesamten virtuellen Wirken gestört wird. Protection richtig verstanden erfordert von Konsumenten das Feingefühl, bei Angriffen in der vernetzten Welt zwischen eher unverfänglichen und schädlichen Bedrohungen unterscheiden zu können, auch wenn wir das physische Sensorium für diese Gegenwehr nicht immer aufbringen.

Preference, oder die Vorlieben von Teilhabern am virtuellen Universum, bezeichnen eine psychologische Orientierung, die auf Produkte, Dienstleistungen und andere Individuen abzielt. Da es einen Überfluss an (Wahl)möglichkeiten im Netz gibt suchen Konsumenten immer nach jenen Positionen die sich im Moment der Suche glücklicherweise ergeben. Sie erflehen geradezu Möglichkeiten, die sich auftun, noch bevor ein bewusstes Bedürfnis nach ihnen besteht. In dieser Welt markieren und repräsentieren die Mausklicks, die Kanalwechsel oder auch die Updates der Aufenthaltsorte, als das aktuelle Verhalten eines Users, wer er im Sinne des Identitätsbegriffes gerade ist. Die Konsumenten können in einer virtuellen Welt durch ihr gelebtes Medienverhalten konkrete Zielangebote auf sich ziehen und so mehr über an den Tag gelegte Präferenzen herausfinden. Andererseits kann das Konsumentenverhalten in der virtuellen Welt ohne weitere Handlungsaufforderung oder Zustimmung des Netzakteurs beobachtet und aufgezeichnet werden. Zielgruppenwerbung im Posteingang ist ein typisches Erscheinungssymptom dieser

netzwirtschaftlichen Praktiken. Daher ist es bedeutsam, dass der Verbraucher ein Bewusstsein dafür entwickelt, dass diese ökonomisch getriebenen Vorgangsweisen Realität des Netzes sind, wenn er Verhaltensweisen Preis gibt.

Natürlich bestehen laut Allison Cerra alle 3 Ps simultan in uns. Während einige sich psychometrisch mehr auf ein P im Besonderen ausrichten machen wir alle mehrmals täglich unwillkürlich bewusste und unbewusste Abstriche von den drei Ps. Die zentralen Fragen in diesem Themenfeld kreisen dann um Abklärungen wie: Soll ich dieses Bild auf meine soziale Netzplattform hochladen? Es kommt darauf an, wie stark ich annehme, dass es für meine Präsentation gegenüber einer bestimmten Zielgruppe von Bedeutung ist. Oder: Soll ich meine Location auf der Social Networking Site updaten? Hier gilt es abzuwägen zwischen dem Schutzanspruch bei Veröffentlichung solcher Informationen und dem Nutzen einer gezielten Interaktion.

Wir sind auch immer von einem der drei Ps zu einer gegebenen Zeit mehr zu motivieren und der Einfluss von Technologien so Revital Marom auf das Paradigma von Generationen ist ebenfalls mit im Spiel, wenn wir unsere Abstriche machen.

Für Revital Marom bilden diese grundsätzlichen Abklärungen ihrer Alcatal Lucent Kollegin zum Verhältnis von Technologienutzung und Generationskultur die theoretische Basis zur Beleuchtung der eigentlichen Frage „Weiß die Elterngeneration was ihre Kinder tun?"

Im heutigen Kommunikationsumfeld, in unserer hyperverbundenen Welt, verschmilzt die Identität eines Konsumenten sehr oft exklusiv mit Bedenken in Bezug auf den Schutz der Privatsphäre. Und die Identität ist ein viel nuancenreicheres Gebilde als Konsumenten oft annehmen. So sind für den richtigen Schutz der Privatsphäre im Netz insbesondere unsere Vorlieben (Präferenzen) und unsere Image-Präsentation verantwortlich.

Revital Marom brachte die ganze Thematik mit ihrer Zentralaussage ziemlich auf den Punkt: „We have a virtual highway, but the drivers have no licence", wir haben eine virtuelle Autobahn, aber die Fahrer haben keinen Führerschein.

Was unsere Kinder angeht, ist dieser Umstand mehr als augenscheinlich. Insbesondere bei Teens, also der Gruppe der 10- bis 19-jährigen, gehört das Zulegen eines bestimmten Images zu den fundamentalen Riten auf ihrem Weg durch die Adoleszenz bzw. die Pubertät. Daher sind die meisten Eltern in diesen schwierigen Jahren sehr verblüfft über die Obsession ihrer Kinder mit Social Networking, mit Gaming oder Ähnlichem. Es ist jedoch klar, dass diese virtuellen Aufenthaltsorte für die Kids die neuen Outlets sind, über die sie sich mit ihren Communities verbinden und ihre eigenen Images pflegen.

Diese Herausforderung wird noch durch das Faktum zusätzlich angeheizt, dass das was Leute (sogar Erwachsene) sagen, sich sehr oft von dem unterscheidet, was sie tatsächlich tun. Die Gründe für diese Diskrepanz wurden von Psychologen über Jahre hinweg studiert und erforscht. Sie verweisen letztlich auf unsere in uns als menschliche Wesen angelegte Tendenz, scheinbar irrationale Verhaltensmuster zu rationalisieren und damit zu rechtfertigen.

Die bei rund 5.000 US-Konsumenten (inklusive einer statistisch signifikanten Kohorte von Teens) durchgeführte Alcatel Lucent Studie lieferte in diesem Zusammenhang interessante Aufschlüsse:

- So identifizierten sich rund 18 % als Privatpersonen, die sehr sorgfältig darauf Acht geben, was sie im virtuellen Raum teilen und wo sie sich mit anderen aufhalten; trotzdem führen rund 50 % dieser Population regelmäßig Updates ihrer sozialen Netzwerkseiten durch mit Details darüber, wo sie gerade sind und wo sie vorhaben zu sein.
- 18 % sind noch umsichtigere Typen, die sich darüber Sorgen machen, übervorteilt zu werden; trotzdem diskutieren 63 % von ihnen persönliche Details über sich selbst wenn sie online sind.
- 11 % sehen die Welt als schaurigen Raum, welcher Umsicht erfordert, um zu vermeiden, dass man selbst oder seine Familien leidvolle Erfahrungen macht bzw. machen; trotzdem gestehen sich 30 % dieser Gruppe ein, dass sie online das genaue Geburtsdatum bekannt geben.

Die Eltern befinden sich daher in einer wenig beneidenswerten Position, wenn es darum geht, was ihre Kinder online tun. In Bezug auf Teens lieferte die Alcatel Lucent Studie nachstehende Hardfacts:

- 75 % haben schon Freundschaftsanfragen (friend requests) akzeptiert oder E-Mails von Leuten beantwortet, die sie nicht gut kennen.
- 73 % haben schon die Wahrheit gedehnt oder ausgeweitet, um ihren Online-Auftritt, ihr Erscheinungsbild im Netz, zu verbessern.
- 60 % haben schon versucht an Leute heranzukommen, die sie online getroffen haben, um Informationen auszutauschen.
- Und 10 % posten regelmäßig Updates, Kommentare oder laden Fotos hoch, wo sie später bereut haben, diese Informationen im Netz zu teilen.

In einer Welt, in der Individuen sich selbst derart freizügig darstellen, heißt die immaterielle Währung die ausgetauscht wird, eigentlich Vertrauen, so die Schlussfolgerung von Revital Marom. Für Konsumenten bringt das Vertrauen, wonach ihr Service-Provider ihre Kundendaten verantwortlich nutzt auch die höhere Bereitschaft mit sich, für identitätsbezogene Dienste zu bezahlen. Für die Eltern

liegt des Rätsels Lösung auch in der Vertrauensfrage. Als Erziehungsberechtigte und Behüter ihrer Kinder müssen sie das heikle Verhältnis abwägen und ausbalancieren, ihren heranreifenden Kindern einerseits größeren Zugang zu Technologie zu ermöglichen und ihre Kinder andererseits vor versteckten Gefahren zu schützen. In der Tat, Vertrauen ist nicht nur die immaterielle Währung zwischen Konsumenten und Service-Betreibern, sondern auch die Währung die im gemeinsamen Haushalt zwischen Eltern und Kindern ausgetauscht wird.

7 „Cyber Security aus Sicht der Jugend”

Dennis WESTHOFF und Max LASSMANN; Schüler des Goethe Gymnasiums, Wien

Die zwei Schüler der Maturaklasse des Goethe Gymnasiums bildeten mit ihrem Vortrag über Cyber Security im Sinne des richtigen Verhaltens im Netz aus Sicht der Jugend den Schlusspunkt des von der GIT im OVE und dem AIT gemeinsam im LIZ der HTL Rennweg veranstalteten ersten „Cyber Security Summits“.

An den Beginn ihrer Ausführungen stellten sie ein paar Anmerkungen zum Wandel der Kommunikationsmedien. Während früher sich die Menschen Briefe schrieben, wenn sie sich was zu sagen oder zu erzählen hatten, wird heute auf verschiedene elektronische Medien zurück gegriffen, die als kleinsten gemeinsamen Nenner eine unheimliche Beschleunigung der Kommunikation mit sich brachten, Egal ob instant Messaging, E-Mail, soziale Netze wie Facebook oder SMS, immer geht es um die unmittelbare Kommunikation, mit der in Sekundenschnelle Nachrichten ausgetauscht werden können, wofür es zuvor Muße brauchte, um seine Gedanken in einen Brief zu fassen.

Danach zeichneten sie den Weg eines E-Mails von einem Laptop über das Wireless Modem und das Netz zum eigenen Mail-Server und dann weiter durch das Labyrinth des Web zu einem Mail-Eingangsserver irgendwo auf der Welt, von wo es schließlich wieder über ein Modem oder einen Router seinen Weg zu einem Empfänger mit seinem Tablett findet. In unserem Zeitalter der alles dominierenden elektronischen Kommunikation haben sich also nicht nur die Mitteilungsmedien geändert, sondern auch die Versandwege zwischen Sendern und Empfängern.

Danach gingen Dennis Westhoff und Max Lassmann auf das größte soziale Netzwerk unserer Tage, auf Facebook ein, welches mit rund 1 Milliarde aktiven Nutzern einen zuvor nie dagewesen Verbreitungsstand erreicht hat, In diesem Netz geben die Nutzer alle Daten freiwillig bekannt: den aktuellen Standort, Fotos, intime Daten wie den Beziehungsstatus und jede noch so kleine Neuigkeit in Form von „Posts“.

Facebook erwirtschaftet mit seinem Geschäftsmodell bei rund 3,7 Milliarden US S Umsatz rund 1 Milliarde US $ Gewinn pro Jahr. Das soziale Netzwerk ist zwar für die Benutzer kostenlos, jedoch nicht gratis, wie die Schüler argumentierten. Die eigenen Präferenzen der Nutzer werden von Facebook mit gnadenloser Profitorientierung für „maßgeschneiderte Werbung“ (targeted advertising) genutzt.

Im Sinne des Generalthemas Cyber Security war es Westhoff und Lassmann danach wichtig zu zeigen wie man sich auf Facebook mit den Privatsphären-Einstellungen zumindest einigermaßen schützen kann. Für alle Statusmeldungen, Fotos oder Informationen, die man mit anderen teilen möchte, lässt sich eine Zielgruppe festlegen. Von Öffentlich, über Freunde bis hin zu benutzerdefinierten Gruppen sehen dann eben nur jene Personen alle Informationen, denen man den Zugang zu diesen Informationen eingeräumt hat. Dies ist insbesondere deswegen von enormer Bedeutung, weil alle Personen mit denen man auf Facebook etwas teilt, diese Informationen einschließlich aller Anwendungen mit anderen teilen können.

Nach jahrelanger harter Kritik an Facebook hat der Betreiber des größten sozialen Netzwerks seinen Benutzern, die schließlich seinen Erfolg ausmachen, ein größeres Recht auf Privatheit zugestanden und die möglichen Privatsphäre-Einstellungen über die zuvor aufgezeigte Zielgruppen-Auswahl für Informations-Sharing weiter verfeinert. Westhoff und Lassmann zeigten, was man hier so alles einstellen kann:

- die Funktionsweise von Verbindungen, wo man bestimmen kann, wie man sich mit bestimmten Freunden verbindet
- Chronik und Markierungen, wo festgelegt werden kann, was mit Inhalten und Beiträgen passiert, die von Freunden in der Chronik markiert werden
- Werbeanzeigen, Anwendungen und Webseiten, wo die entsprechenden Einstellungen für Werbeanzeigen, Anwendungen, Spiele und Webseiten verwaltet werden können
- Beschränkung des Publikums für ältere Beiträge, womit man Zugangseinschränkungen für Beiträge festlegen kann, die man mit Freunden von Freunden oder der Öffentlichkeit geteilt hat

und zu guter Letzt

- Blockierte Personen und Anwendungen, womit man die Möglichkeit erhält, blockierte Personen und Anwendungen zu verwalten.

Am Ende ihres Streifzuges durch Facebook übten die Schüler noch weitere Kritikpunkte die man im Umgang mit diesem Medium nicht aus den Augen verlieren sollte. Sie alle zeigen, wie sehr wir uns dem „gläsernen Menschen“ schon genähert haben. Auf Facebook erfolgt die Registrierung anonym, die Daten von Mitgliedern werden zeitlich unbegrenzt genutzt und alle Inhalte dürfen kommerziell verwendet und an Dritte weiter gegeben werden. Bei der Facebook-Integration in Smartphones kommt noch erschwerend hinzu, das Facebook auf das Adressbuch zugreift. Selbstverständlich werden Facebook-Veröffentlichungen sowohl von Nachrichtendiensten und der Polizei ausgewertet und auch in der Arbeitswelt werfen Human Resources Abteilungen bei Bewerbungen und Besetzungen immer mal wieder einen Blick in Benutzerprofile auf Facebook. Einer der am schwersten

wiegenden Kritikpunkte ist aber sicherlich das erschwerte Löschen des eigenen Benutzerkontos wenn jemand aus diesem sozialen Netzwerk wieder aussteigen möchte.

Warum dann trotzdem fast alle jungen Menschen auf Facebook sind, erklären sich die Schüler so: Das Medium ist praktisch, man hat es immer dabei, man kann organisatorische Dinge schnell lösen, Kontakte halten und alte Freunde wieder finden. Die Argrumente sind mehr als nachvollziehbar, doch es bleibt auch Vorsicht geboten.

Doch Facebook ist im Leben von Jugendlichen nur ein Medium welches mehr Beachtung in Bezug auf Sicherheit verdient, so die Schüler. Das zweite ist natürlich das Smartphone, „die Gefahr in der Hosentasche" wie Westhoff und Lassmann dies nannten. Das Handy ist heute längst ein vollwertiger Computer, bei dem es aber noch schwerer als bei Tabletts und Laptops fällt, immer die Transparenz im Blick zu haben. Durch eingeschaltetes GPS-Tracking kann man eigentlich mit Smartphones immer geortet werden. Die laufende Synchronisation von Kontakten, Terminen, Mails, Notizen über „Clouds" vermehrt die Angriffsflächen auf intime Daten um ein Vielfaches wie auch schon an anderer Stelle bei diesem Summit zu hören war. Und natürlich sind die heutigen Smartphones z.B. mit geladenen Apps für Mitgliedskarten auch wunderbare Zielscheiben für die Auswertung des Kaufverhaltens der Anwender. Der Rat der Schüler: Auch bei diesen Kleincomputern zumindest elementare Sicherheitsüberlegungen anstrengen.

Zum Schluss ihres in Tandem-Präsentation gestalteten Vortrages machten die Maturaschüler noch einen Abstecher auf die große Bühne der europäischen Politik von der ihrer Meinung nach auch Ungemach im Sinne der totalen Einsicht in die Privatsphäre droht. Als Beispiel brachten sie eine Schlagzeile aus „DIE ZEIT": „EU-Kommission reicht Klage gegen Deutschland ein". Der Hintergrund: Deutschland hat die Europäische Richtlinie zur Vorratsdatenspeicherung von 2006 nicht umgesetzt. Diese bildet aber die Rechtgrundlage dafür, Telefon- und Internetdaten unter der Begründung vorbeugender Kriminalitäts- und Terrorismusbekämpfung für 6 Monate zu speichern. Hier sind wir wieder beim Keynote-Speaker, der den ewig währenden Konflikt zwischen Sicherheits- und Freiheitsbedürfnis ebenso mit Beispielen in den Mittelpunkt der Diskussion gestellt hat.

Mit dem bewusst provozierenden Schlusswort „Was kann man dagegen tun?" leiteten die beiden Schüler nach ihrer Darbietung spannender Einsichten in Medienwelten von Jugendlichen in die allgemeine Abschlussdiskussion des Cyber Security Summit über.