TECHNISCHE UNIVERSITÄT WIEN
Vienna University of Technology
Fachbereich Rechtswissenschaften

Gerald Schnepf, 0126175

Präventive Methoden gegen Cyberstalking

Bakkalaureatsarbeit

Ass.-Prof. Mag. et Dr. iur. Markus Haslinger

Seminar (mit Bakkalaureatsarbeit)

Januar 2012

Inhaltsverzeichnis

Allgemeines über Cyberstalking

Das Internet begann als Zusammenschluss verschiedener nationaler Militär- und Forschungsnetzwerke in den frühen 80er Jahren. Nachdem die ersten kommerziellen Internet Service Provider Mitte der 90er Jahre gegründet wurden, wuchs die Anzahl der verbundenen Rechnern rasant an. Lange Zeit war das Internet ein Ort für Computerenthusiasten und zeichnete sich durch gesellschaftliche Abgeschiedenheit aus, doch durch flächendeckende Vernetzung und vereinfachten Benutzerschnittstellen wurde das Internet auch zunehmend für den privaten und kommerziellen Gebrauch verwendet. Junge Geschäftsleute erkannten den Wert und Möglichkeiten der globalen Vernetzung und das Internet erlebte einen kurzweiligen Boom, der heutzutage als Dotcom-Blase bekannt ist, die im Jahr 2000 platzte und viele kleinere und mittlere Unternehmen in den Bankrott trieb.

Heute wird das Internet für eine Vielzahl von sozialen Anwendungen verwendet. Spiele wie Ultima Online von Elektronic Arts, Valve's Counter-Strike, Blizzard's World of Warcraft oder Zynga's Farmville wurden durch den Netzwerkaspekt zu einer virtuellen Plattform für soziale Interaktion. Soziale Webseiten wie Geocities, Tripod, Myspace, Facebook und Youtube forderten die Benutzer zur Interaktion auf, in Chatrooms oder durch Verteilung selbsterstellter Inhalte. Doch das Teilen von Inhalten ist nicht nur auf das Teilen von bewusst erstellten Inhalten begrenzt. Aufgrund der Fülle an geteilter Information können auch Gewohnheiten, Vorlieben oder andere private Daten herausgelesen werden.

Stalking, das obsessives Verfolgen von Personen gepaart mit Belästigungen und Bedrohungen, ist lange nicht mehr nur ein Problem von Prominenten. Privatpersonen werden oft Opfer von beharrlichen Verfolgern. Viele davon aus dem eigenen sozialen Umfeld; Ex-Liebschaften, Bekannte, Arbeitskollegen, Freunde oder gar Familienmitglieder. Durch verstärkte Verwendung des sozialen Aspekts des Internets werden zunehmend auch neue Möglichkeiten der Verfolgung möglich.

Stalking (damit auch Cyberstalking) gilt aus kriminologischer Sicht als eskalierendes Verhalten. In der Praxis werden Kapitalverbrechen oft von Stalking im Vorfeld begleitet.

Diese Arbeit beschäftigt sich mit präventiven Verhinderung von Cyberstalking-Fällen. Dabei handelt es sich vor allem um technische Methoden, die einem Cyberstalker sein Werk stark erschweren soll.

Statistiken

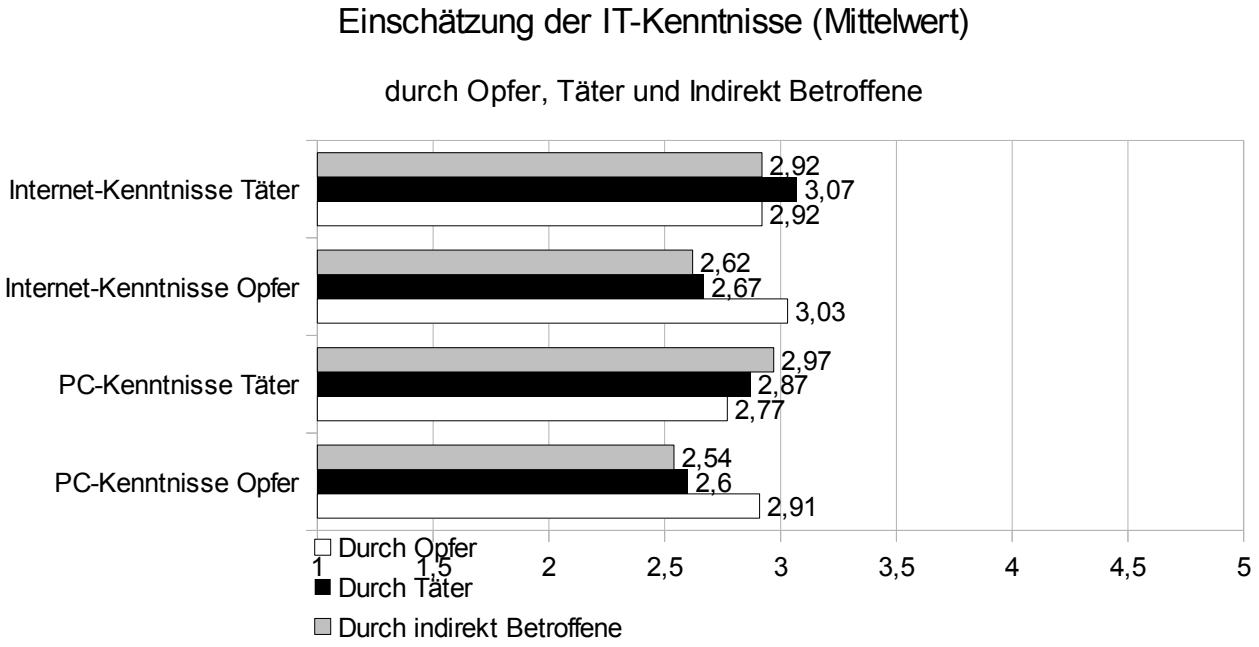
Statistiken aus Österreich

In Österreich werden jährlich etwa 2500 Stalkingfälle gemeldet, dies inkludiert nicht die Fälle von Stalking als Auftakt zu einem Kapitalverbrechen. In 80% der Fälle sind die Täter männlich, die Aufklärungsrate ebenfalls liegt bei etwa 80%. Cyberstalking ist nicht in einem einzelnen Paragraphen festgehalten, weshalb genaue Zahlen schwierig zu ermitteln sind.

In einer österreichischen Studie[1], die von 2005 – 2007 aktiv war, wurden Eckdaten für Cyberstalking in Österreich aufgestellt. Insgesamt basiert die sie auf 103 Datensätzen (75 Opfer, 13 indirekt Betroffene, 15 Täter).

Geschlecht	Täter Weibl.	Täter Männl.
Opfer Weibl.	19	59
Opfer Männl.	17	8

Herkunft	Opfer	Täter	Indirekt[2]
Österreich	21	3	6
Deutschland	51	11	7
andere	3	1	0



Die Grafik zur Einschätzung der IT Kenntnisse zeigt eine deutliche Überschätzung der Opfer bei ihren eigenen PC- und Internet-Kenntnissen. Täter

1 Cornelia Belik – Cyber stalking Ergebnisse einer Onlinebefragung, 2007 Books on Demand GmbH, ISBN 978-383-700-849-4

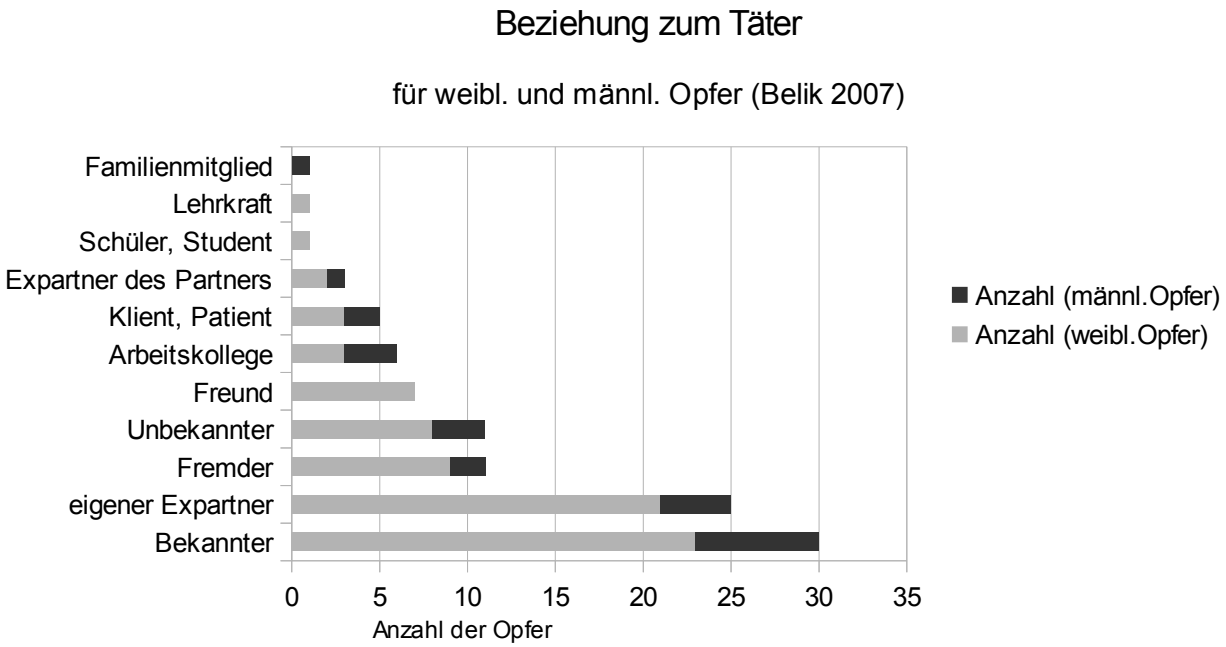
2 Indirekt steht hier für „Indirekt Betroffene“, also weder Opfer noch Täter. zB. eine Vertrauensperson des Opfers

überschätzen sich möglicherweise geringfügig, werden aber von Opfern bei ihren PC-Kenntnissen deutlich unterschätzt.

Belästigungen	erste	häufigste
E-Mail	41	40
Foren	15	15
SMS	11	11
Webseite	7	5
Instant Messenger	6	11
Chat	6	7

Belästigungen	erste	häufigste
Daten im Internet	4	7
anzügl. Fotos	3	1
Mailingliste	2	2
Blogs	1	3
Newsgroups	1	0
Einkäufe	1	0

Bei den Formen von Belästigung ist die Email klarer Favorit. Foren-, Chat und Virenbelästigung kommt meist eher von weniger Bekannten oder Unbekannten. Im engeren Umfeldsind meist SMS oder Instant Messenger der Favorit, aber auch die Veröffentlichung von Daten im Internet (zB. Fotos).



Die Graphik „Beziehung zum Täter“ zeigt häufiges Stalkingverhalten bei Expartnern (sum. 25) und gelegentlichen Kontakten (sum. 30). In 22 Fällen (Unbekannte bzw. Fremde) gab es keine sichtbare Beziehung, bevor es zu einem Cyberstalking-Fall kam.

Statistiken aus den USA

Zum Vergleich und die Datenentwicklung zu zeigen, werden hier zusätzlich Statistiken aus den USA[3] angeführt. Die Stichprobengröße ist hier um ein Vielfaches höher und sie wird zudem jährlich seit 2000 geführt.

Dienst	Verlauf	μ
E-Mail	39,50% → 34,00%	**37,25%**
Forum	17,50% → 9,50%	**13,81%**
Instant Messenger	13,00% → 6,00%	**12,35%**
Chat	15,50% → 2,50%	**7,74%**
Webseite	7,50% → 4,50%	**6,35%**
Facebook	5,50% → 16,50%	**11,00%**
Telefon	7,00% → 6,25%	**5,25%**
Myspace	5,50% → 4,50%	**5,17%**
Dating Plattformen	2,50% → 1,25%	**1,88%**
Craigslist	2,50% → 1,50%	**2,00%**
SMS	2,50% → 4,50%	**3,50%**
Spiele Plattformen	2,50% → 0,25%	**1,38%**

μ: arthmetisches Mittel (Mittelwert)
Craigslist: amerikanische Kleinanzeigenseite

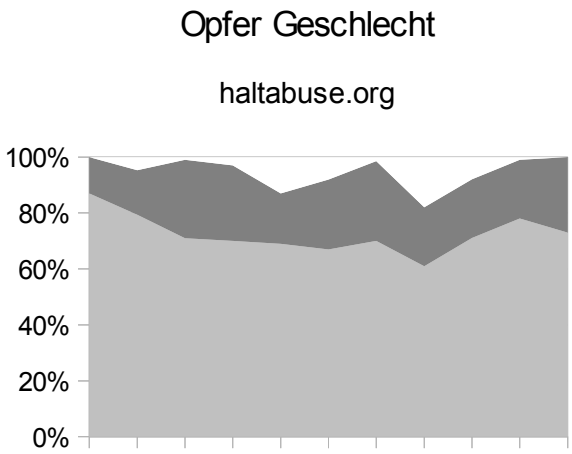
Bei einem Vergleich der von Cyberstalkern benutzten Diensten, sind ähnliche Verhältnisse wie in Österreich zu erkennen. Email ist deutlich an erster Stelle, Foren und IM an zweiter.

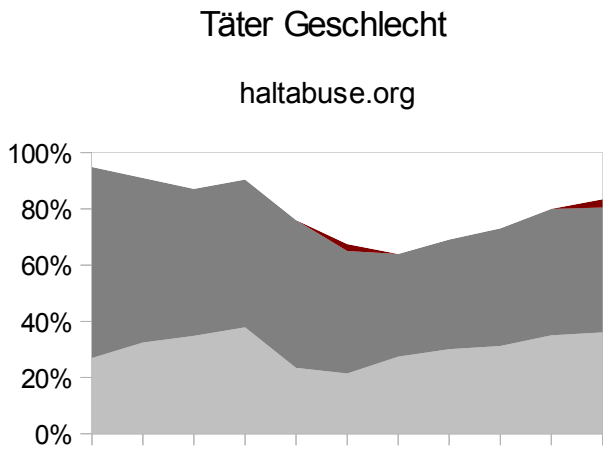
Anzumerken ist, dass auf Facebook ein rasanter Anstieg verzeichnet wird, seit es in die Statistik aufgenommen wurde (2009). 2010 wurden 16,5% der gemeldeten Cyberstalking-Fälle hauptsächlich auf dieser Seite begangen.

Die Tabelle „Beziehung Täter – Opfer“ zeigt bei den in den USA gemeldeten Studien ein anderes Verhalten als die österreichische Statistik. Hier liegt deutlich der unbekannte Täter an erster Stelle gefolgt von ehemaligen Liebes-beziehungen.

Beziehung Täter – Opfer	2000	2002	2003	2004	2005	2006	2007	2008	2009	2010	TOTAL
keine	53%	41%	42%	54%	51%	52%	56%	43%	39%	53%	1506
Exfreund/in	12%	17%	33%	24%	17%	23%	14%	26%	26%	26%	591
Freund/in	13%	9%	12%	4%	5%	6%	6%	3%	5%	3%	191
Arbeitskollege	0%	5%	5%	3%	6%	3%	3%	4%	5%	4%	104
Online Bekanntschaft	0%	17%	4%	9%	13%	12%	12%	5%	13%	6%	264
Schule	0%	1%	3%	3%	2%	2%	0%	0%	2%	2%	45
Familie	12%	2%	1%	2%	2%	2%	6%	5%	9%	3%	124
Online Exfreund/in	0%	0%	0%	0%	3%	0%	0%	11%	0%	0%	38
andere	10%	8%	0%	0%	1%	0%	3%	4%	1%	4%	198

3 Quelle: WHO@ cumulative statistics http://www.haltabuse.org/resources/stats/index.shtml (abgerufen: Jänner 2012)





Opfer Geschlecht	Weibl.	Männl.	Unbekannt
2000	87,00%	13,00%	0,00%
2001	79,30%	16,00%	4,70%
2002	71,00%	28,00%	1,00%
2003	70,00%	27,00%	3,00%
2004	69,00%	18,00%	13,00%
2005	67,00%	25,00%	8,00%
2006	70,00%	28,50%	1,50%
2007	61,00%	21,00%	18,00%
2008	71,00%	21,00%	8,00%
2009	78,00%	21,00%	1,00%
2010	73,00%	27,00%	0,00%
µ	**72,39%**	**22,32%**	**5,29%**

Täter Geschlecht	Weibl.	Männl.	Gruppen	Unbekannt
2000	27,00%	68,00%	0,00%	5,00%
2001	32,50%	58,60%	0,00%	8,90%
2002	35,00%	52,00%	0,00%	13,00%
2003	38,00%	52,50%	0,00%	9,50%
2004	23,50%	52,50%	0,00%	24,00%
2005	21,50%	43,50%	2,50%	32,50%
2006	27,50%	36,50%	0,00%	12,20%
2007	30,00%	39,00%	0,00%	31,00%
2008	31,00%	42,00%	0,00%	27,00%
2009	35,00%	45,00%	0,00%	20,00%
2010	36,00%	44,50%	3,00%	16,50%
µ	**30,64%**	**48,55%**	**0,50%**	**18,15%**

Die geschlechtsbezogene Statistik zeigt ähnliche Zahlen wie die Österreichischen. Als gemeldete Täter kommen eher Männer in Frage (fast 50%), als hilfesuchende Opfer häufig Frauen (über 70%).

Die Zahlen fluktuieren sehr stark. Die Zahl der männlichen Täter ging seit 2001 deutlich zurück, aber die Zahl der Täter unbekannten Geschlechts erhöhte sich.

Interviews

Um etwas tiefere Einsicht in den Sachverhalt zu bieten, wurden auch Erfahrungen von erfahrenen Nutzern einbezogen.

Interview mit K

1. **ASL** (Alter, Geschlecht, Wohnort)

   23, Weiblich, Wien

2. **Wie gut kennen Sie sich - nach persönl. Einschätzung - mit dem PC/Internet aus?**

   Ausreichend. Ich meine dass ich meinen PC vor schädlicher Software/Viren schützen kann und weiß welche Hardware in meinem PC verbaut ist und wie ich daran was repariere. Ich hab meinen eigenen PC mit 10 bekommen und bin mit dem Internet groß geworden da wir seit 1999 Internet haben

3. **Verwenden Sie Social Networks (zb. Facebook)?**

   Ja, mehrere Accounts auf unterschiedlichen Namen. Gaming-Account zum Spielen um im Spiel erfolgreicher zu sein, aber die Leute sollen keine Privatinformation über mich haben. Wenn ich Leuten böse nachreden wollen würde, würde ich auch dafür eigene Accounts anlegen.

4. **Wie oft verwenden Sie das Internet und wofür?**

   Täglich, für Social Networking. Spiele (MMORPG), Facebook, Twitter, Emails, Online-Banking

5. **Wissen Sie, was Cyber Stalking ist?**

   JA

6. **Sind Sie schon einmal Opfer eines Stalkings geworden?**

   Nein, lasse ich nicht zu

7. **Sind Sie schon einmal als Täter aktiv geworden?**

   Ja

8. **Wie alt waren Sie dabei?**

   21-22

9. **Kannten Sie das Opfer?**

   Natürlich, mein Ex-Freund

10. **Geschätztes Alter des Opfers?**

    30

11. **Geschlecht des Opfers?**

    Männlich

12. **Wie haben Sie gestalkt?**

    Mail, Facebook, Online-Banking

13. **Wie lange dauerte das Stalking an?**

    Ein halbes Jahr, alle 3-4 Tage Facebook, Email und Online-Banking ganz selten

14. **Haben Sie auch Maßnahmen verwendet um unerkannt zu bleiben?**

    Ich habe den Ghost/Stealth-Modus aktiviert (wenn der Onlinedienst das zuließ) und/oder bin über Proxys gegangen. Gemerkt hat er es nie. Außerdem hab ich meine Passwörter nach unserer Trennung geändert, er hat das nie. Und wenn du seit 10 Jahren immer die gleichen Passwörter benutzt, dann kennt die der Partner nach 6 Jahren halt auch.

15. **Haben Sie sich je als ihr Opfer ausgegeben?**

    Ich habe nie etwas aktives gemacht. Dann ist ja die Gefahr das es rauskommt, das würde den ganzen Spaß verderben. Es ist ja gerade lustig wenn er nicht weiß, dass jemand mitliest, wenn er ungehemmt alles schreibt.

16. **Beziehung zu Opfer?**

    Ex-Partner

17. **Wodurch hat das Stalking aufgehört?**

    Interesse verloren, mit der Beziehung abgeschlossen, aber ab und zu schau ich immer noch rein .. zum Spaß

18. **Haben Sie noch Kontakt zum Opfer?**

    Nja, selten

19. **Finanzielle Schäden?**

    Für mich ja, deswegen Stalking. Ich bin aus der Beziehung mit finanziellem Verlust rausgegangen und hatte ein Rachegefühl. Es verschaffte mir Genugtuung zu sehen dass sein neues Leben nicht besser, eher schlechter ist, als mit mir.

20. **Kennen Sie andere Opfer?**

    Ja, eine Schulfreundin ist bei einem Treffen mit einem Cyberstalker vom Täter ermordet worden. Er hatte viele Mädchen wahllos angeschrieben und sich dabei selbst als Frau ausgegeben.

Interview mit W

1. **ASL** (Alter, Geschlecht, Wohnort)

   31, Weiblich, Wien

2. **Wie gut kennen Sie sich - nach persönlicher Einschätzung - mit dem PC/Internet aus?**

   Gut, mit Hardware kenn' ich mich nicht so gut aus, Zusammenbauen könnte ich, wenn ich die einzelnen Teile parat habe, aber der Knackpunkt ist ja die Auswahl der Teile (das lässt man andere machen ☺). Virenscanner und Adware-Blocker verwende ich, der Router im Heimnetzwerk hat eine integrierte Firewall, die ein Freund meines Freundes eingerichtet hat.

3. **Verwenden Sie Social Networks (zB. Facebook)?**

   Ja, nur Facebook. „Sicheres Browsing“ hab ich eingestellt (zum Leidwesen einiger Spiele) und einige Daten sind nur für Freunde verfügbar. Ich verwende FB eher zum Spielen.

4. **Wie oft verwenden Sie das Internet und wofür?**

   Täglich, FB für Kontakte mit Verwandten (die ich sonst nicht mehr erreichen konnte). Spiele, Chat, Einkaufen, Foren, Suchen(Spaß/Spiel/Weiterbildung), .. für was eigentlich nicht

5. Wissen Sie, was Cyberstalking ist?

Ja

6. Sind Sie schon einmal Opfer eines Stalkings geworden?

Ja, mein Ex-Freund war immer dann auf einer Webseite online wenn ich auch gerade da war, und wusste immer was ich geschrieben hatte. Hatte damals einen Verdacht, ob er nicht einen Trojaner auf meinem Computer installiert hat. Er kannte sich damit aus.

7. Sind Sie schon einmal als Täter aktiv geworden?

Nein, ich hab niemanden genervt, nicht mal mit Emails

8. Wie alt waren Sie dabei?

21

9. Kannten Sie den Täter?

Ja, Ex-Freund. Nachdem ich ihn nach einem physischen Übergriff vor die Tür gesetzt habe.

10. Geschätztes Alter des Täters?

19

11. Geschlecht des Opfers?

Männlich

12. Wie wurden Sie gestalkt?

In Chats, sogar 3 verschiedene. Irgendwie war ich aber froh dass er „nur“ online nachstellte und nicht vor meiner Tür auftauchte.

13. Wie lange dauerte das Stalking an?

Ein halbes Jahr

14. Hat er Maßnahmen verwendet um unerkannt zu bleiben?

Er nicht, wollte er auch nicht.

15. Haben er sich je als Sie ausgegeben?

Nein

16. Beziehung zu Opfer?

Ex-Partner, aber er verfolgte mich nicht um mich zurückzubekommen, sondern aus Rache

17. Wodurch hat das Stalking aufgehört?

Ganz plötzlich war er weg. Vielleicht hat jemand anderer ihn angezeigt, ich weiß es nicht.

18. Haben Sie noch Kontakt zum Opfer?

Nein

19. Finanzielle Schäden?

Nein

20. Kennen Sie andere Opfer?

Die Ex-Partnerin meines Ex-Freundes, bei ihr ist ähnliches vorgefallen.

Präventive Methoden

Neben rechtlicher Initiativen ist Cyberstalking teilweise auch ein technisches Sicherheitsproblem. Wenn ein Übeltäter technischen Zugang zu einem System besitzt, können die Folgen vielschichtig sein. Abgesehen vom technischen Schaden kann einem Opfer auch auf finanzieller, sozialer und psychischer Ebene geschadet werden.

Der folgende Abschnitt ist in Unterkapitel geteilt.

- Im Kapitel **Computersicherheit** werden Methoden zur Sicherung des eigenen PCs aufgeführt.
- Im Kapitel **Datensicherheit** geht es um Methoden zum Sichern der eigenen Daten.
- **Netzwerksicherheit** beschäftigt sich mit Absicherung des eigenen Netzwerks, insbesondere eines kabellosen Netzes (WLAN)
- **Verhalten im Internet** soll Methoden zur sicheren Verwendung des Onlinemediums bereitstellen.

Computersicherheit

> *I think computer viruses should count as life. I think it says something about human nature that the only form of life we have created so far is purely destructive. We've created life in our own image.* — Stephen Hawking

Computersicherheit wird hier als Sicherheit vor dem Ausfall eines einzelnen Computersystems geführt. Das bedeutet daß ein System, dass keine technischen Mängel aufweist, korrekt funktioniert ohne von Viren, Trojanern oder anderer Malware beeinflusst zu werden.

System-Updates

Das Betriebssystem eines Computers (wie Windows, Linux, MacOS) kann Fehler enthalten, die den Computer anfällig für Hacking-Angriffe machen. Solche Sicherheitslücken können, sobald sie bekannt sind, innerhalb von kurzer Zeit geschlossen werden.

Für den Anwender äußert sich das als Bereitstellung eines Aktualisierungspakets (oder System-Update), dass meist schnell und gratis von der Homepage des Betriebssystem-Herstellers bezogen werden kann.

Antivirus-Software

Antivirus-Software prüft die installierten Anwendungen sowie Dokumente, Bilder und andere Dateien auf verdächtiges Verhalten bzw "Aussehen" und kann so den Anwender auf Infizierung mit einem Virus hinweisen bzw. Gegenmaßnahmen einleiten.

Ein Virenscanner schützt nur dann vor Malware[4] wenn er sie kennt, also die Signatur zur Verfügung steht. Da immer wieder neue Arten von Malware entwickelt werden, aktualisieren die Hersteller von Antiviren-Software immer wieder Ihre Methoden zur Malware-Bekämpfung.

Für den Anwender äußern sich das als Programm-Update oder Aktualisierung der vorhandenen Signaturen. Die meisten Virenscanner machen das automatisch, wenn eine Internetverbindung besteht.

Firewall

Eine Firewall dient dazu, den eingehende und ausgehenden Datenverkehr zu überwachen und, falls notwendig, zu filtern. Einerseits ist es für einen Angreifer schwieriger einen geschützten Computer von Außen anzugreifen (sprich: zu hacken), andererseits ist es für Malware schwieriger, durch eine Firewall mit einem Angreifer zu kommunizieren wenn sie von einer Firewall und in Folge vom Anwender bemerkt wird.

4 Sammelbegriff für alle Formen schädlicher Software (Viren, Trojaner, Würmer, ...)

Eine Firewall ist keineswegs ein Ersatz für eine Antiviren-Software, obwohl sie vor einigen Formen von Schadsoftware schützen kann.

Browser

Ein Browser (wie Internet Explorer, Firefox, Google Chrome, Opera oder Safari) ist ein Portal zum Internet. Es lädt Dokumente, Bilder und andere Dateien von anderen Computern und setzt sie zu Webseiten zusammen. Da in einigen Dateien Schadsoftware versteckt sein kann, die darauf ausgelegt ist den Browser zu infizieren, sollte auch hier regelmäßig aktualisiert werden.

Außerdem speichern die meisten Webbrowser den Verlauf besuchter Webseiten sowie Formulardaten und Cookies (kleine Dateien, die von Webseitenbetreibern angelegt werden können). Gerade auf fremden Computern sollte darauf geachtet werden, diese Spuren nach Verwendung des Browsers zu löschen oder den Modus *„Privates Surfen“* zu verwenden um eine Aufzeichnung solcher Daten zu verhindern. Viele Browser unterstützen auch das automatische Löschen der Cookies nach dem Schließen des Browser-Programms.

Gäste-Account

Gerade wenn ein Computer von mehreren Personen verwendet wird, ist es oft sinnvoll, ein stark eingeschränktes Konto für etwaige Gäste einzurichten. Ein Gast darf beispielsweise nur den Browser verwenden, Musik abspielen oder Bilder ansehen, aber keine Ihrer privaten Dokumente lesen oder gar neue Anwendungen installieren.

Datensicherheit

Those who do not archive the past are condemned to retype it!
— Garfinkel and Spafford, Practical UNIX Security (first edition)

Datensicherheit soll persönliche oder wichtige Daten vor allem vor Verlust, Manipulationen und unberechtigter Kenntnisnahme durch Dritte schützen.

Mögliche Gefahrenquellen

- **Höhere Gewalt wie Feuer oder Blitzschlag**

  Gegen Naturgewalten die den Computer physisch beschädigen, kann man nur wenig tun, wenn es erst mal zu spät ist. Hier helfen nur Maßnahmen im Vorfeld.

- **Fehlbedienung durch Anwender**

  Bei Bedienung eines Computers kann es zu menschlichen Fehlern durch Anwender kommen. Wichtige Dokumente könnten versehentlich unwiederbringlich gelöscht werden oder eine versehentlich ausgelöste Tastenkombination richtet schweren Schaden an.

- **Viren, Trojaner und andere Malware**

  Malware kann einen Computer und auch alle ein- und ausgehenden Daten infizieren. Selbst Backups können noch verseucht sein, weshalb viele Firmen mehrere Backup-Routinen parallel anwenden (zB. Täglich, Wöchentlich und Monatlich) um selbst im Falle von schwerwiegenden IT-Problemen immer eine Kopie ihrer Firmendaten zu haben.

- **Phishing und Social Engeneering**

  Unter Phishing versteht man die Praxis über gefälschte Nachrichten zur Eingabe von sensiblen Nutzerdaten (zB. für OnlineBanking) verführt zu werden. Social Engeneering ist das Verwenden von sozialer Manipulation um an geheime Daten des Ziels zu kommen.

Gegenmaßnahmen

- **regelmäßige Datensicherung auf externen Datenträgern**

  Das Erstellen von Sicherungskopien erlaubt das Wiederherstellen von Datenbeständen. Leider wird im privaten Bereich oft auf regelmäßige Backups verzichtet, obwohl zu diesem Zweck eine Vielzahl an Lösungen (kommerziell und gratis) zur Verfügung stehen. Manche Lösungen bieten auch einen Speicherplatz auf einem entfernten Rechner an um dort seine Backups zu hinterlegen.

- **Überspannungsschutz**

  Zur Absicherung vor Stromschwankungen und Stromausfällen verwenden kommerzielle Betreiber oft Anlagen zur unterbrechungsfreien Stromversorgung (USV), die auch im Falle eines Stromausfalls für bis zu einer Stunde die Stromzufuhr sicherstellen. Für nicht-kritische Systeme reicht aber ein Überspannungsschutz in der Regel aus.

- **kompromittierte[5] Systeme von Schadsoftware säubern**

  Wenn Malware erfolgreich in das System eingeschleust wurde, ist manchmal auch die Sicherheitssoftware (Virenscanner, Firewall,..) infiziert. Um hier Abhilfe zu schaffen, bieten einige Hersteller Live-Systeme an die von CD oder USB-Speicherstick gestartet werden können um dann auf dem Computer nach Malware zu suchen, ohne von dem infizierten Softwaresystem abhängig zu sein.

- **eingeschränkte Benutzerrechte verwenden**

  Bei Linux und MacOS wird für administrative Tätigkeiten ein eigener Account mit eigenem Passwort verwendet. Ein potenzieller Angreifer kann ohne administrative Rechte keine grundlegenden Systemänderungen durchführen, was den angerichteten Schaden zu einem gewissen Maß eindämmt.

- **sensible Daten verschlüsseln**

  Sensible Daten (wie Passwörter, persönliche Briefe, Bewerbungen, eingescannte Dokumente, private Fotos oder Videos) sollten erst nach Eingabe eines Passworts eingesehen werden können. Das verhindert, dass ein Trojaner die unverschlüsselten Daten an Dritte weiterleitet oder überhaupt findet.

5 Als kompromittiert gelten Computersysteme, wenn sie möglicherweise von Malware betroffen sind.

Netzwerksicherheit

> *Security in IT is like locking your house or car – it doesn't stop the bad guys, but if it's good enough they may move on to an easier target.* — Paul Herbka

Netzwerksicherheit setzt sich mit Sicherheit von mehreren verbundenen Rechnern auseinander. Obwohl das Internet nur ein Zusammenschluß unzähliger lokaler Netzwerke ist, wird der Fokus hier auf Sicherheitsmaßnahmen für das eigene lokale Netzwerk liegen.

Aufbau

Ein Netzwerk besteht meist aus folgenden Bestandteilen:

- **einem Router**: sorgt für die Kommunikation zwischen den Rechnern im Netzwerk
- **einer beliebigen Anzahl von Server** (zB für Netzlaufwerke, Drucker)
- **einer beliebigen Anzahl an Client-Computer** für die Anwender

Für Privatanwender werden spezielle Geräte angeboten die gleichzeitig die Funktion eines Routers übernehmen und jedem Rechner im Netzwerk Zugang zum Internet gewähren (meist schlicht Modem genannt). Diese Geräte haben den Vorteil dass nur wenige oder gar keine Einstellungen verändert werden müssen, aber den Nachteil dass einige Einstellungen nicht zugänglich sind und nur langsam Sicherheitsupdates erfahren.

WLAN

Viele Benutzer besitzen ein Netzwerk ohne dass sie es wissen. Wenn im eigenen Zuhause ein kabelloses Netzwerk (WLAN) betrieben wird, sollten auch Maßnahmen zur Sicherung angestrebt werden.

Außer der Wahl des WLAN-Passworts und des verwendeten Verschlüsselungsstandards sollte auch beachtet werden, dass der WLAN-Router nur über LAN (nach Anschließen eines Netzwerkkabels) konfiguriert werden kann. Dadurch kann niemand den Router per Funk steuern, was einen deutlichen Sicherheitsgewinn bedeutet.

Wie bei allen Passwörtern sollte auch das WLAN-Passwort möglichst lange und komplex sein. Es sollte auch nicht mit dem Passwort für die Konfiguration des Routers übereinstimmen.

Verschlüsselung

Die meisten Hersteller von WLAN-Router sind inzwischen dazu übergegangen, standardmäßig WPA[6]-Verschlüsselung zu aktivieren und ein ausreichend gutes Passwort zu verwenden, das auch auf dem Gerät selbst vermerkt ist. Leider sind auch diese Passwörter nicht so sicher wie es scheint, da sie beim Hersteller gesammelt aufliegen, wodurch ein Besitzer der Datei einen

6 Wi-Fi Protected Access, Verschlüsselungsmethode für drahtlose Netzwerke

erfolgreichen Angriff wesentlich leichter durchführen kann. Deshalb sollte auch dieses Standard-Passwort geändert werden.

WPA ist bis auf eine Sicherheitslücke aus dem Jahr 2008 ausreichend sicher. In WPA2 wurde im Jahr 2010 eine Sicherheitslücke entdeckt. Beide Lücken haben die Eigenschaft, dass sie das Erraten des WLAN-Passworts zwar erleichtern, aber keine anderen Maßnahmen (zB. Aufzeichnen des Datenverkehrs von anderen Rechnern im Netzwerk) zulassen.

WEP[7]-Verschlüsselung bietet nur geringen Schutz vor Angriffen und sollte zugunsten von WPA oder WPA2 aufgegeben werden, da WPA zusätzlich temporäre Schlüssel (TKIP) einführte, die für jedes Datenpaket gewechselt werden. In WPA2 wurde dieses Konzept zusätzlich erweitert (CCMP) und mit verbesserten Verschlüsselung (AES) und stärkeren Schlüsseln (128 statt 64 Bit) aufgewertet.

Unsichere WLANs (unverschlüsselte bzw. WEP-verschlüsselte) haben nicht nur den Nachteil, das jeder das Netzwerk einsehen kann. Unberechtigte können auch alle Daten zwischen Computer und Router mitlesen. Wenn Seiten oder Emails mittels HTTPS oder anderen abgesicherten Protokollen abgerufen werden, wird die Sicherheit jedoch geringfügig erhöht.

7 Wired Equivalent Privacy - Verschlüsselungsmethode für drahtlose Netzwerke, gilt aufgrund von verschiedenen Schwachstellen als unsicher

Verhalten im Internet

Amateurs hack systems, professionals hack people. — Bruce Schneier

Datensparsamkeit

Datensparsamkeit ist ein Begriff aus dem Bereich Datenschutz und soll den Internetnutzer zu sorgfältigem Umgang mit seinen personenbezogenen Daten bewegen.

Definition

Die Grundidee der Datensparsamkeit hängt eng mit dem Begriff der Erforderlichkeit zusammen. Demnach sollen nur so viele Daten mitgeteilt, verarbeitet und gespeichert werden wie für die Lösung der gestellte Aufgabe erforderlich sind, nicht mehr.

Außer der rechtlichen Durchsetzung erfordert eine sinnvolle Implementierung auch technische Mitarbeit seitens der Systemdesigner bzw. der IT.

Datensparsamkeit richtet sich an den Anwender. Dieser soll nicht freiwillig mehr Daten bereitstellen, als notwendig sind, da hierdurch seine Privatsphäre irreparabel geschädigt werden könnte.

Rechtliche Situation

In Deutschland besagt §3a Bundesdatenschutzgesetz, dass nur so viele personenbezogene Daten von einem Serviceprovider erhoben werden dürfen wie für die Bereitstellung des Service notwendig sind, soweit dies keinen unverhältnismäßigen Aufwand seitens des Serviceproviders bedeutet.

Das heißt, dass beispielsweise ein Email-Provider an sich nicht die reale Wohnadresse verlangen darf, da es für die Bereitstellung eines einfachen Email-Kontos nicht notwendig ist. Viele Email-Anbieter

In Österreich und der Schweiz ist Datensparsamkeit und Erforderlichkeit nicht wörtlich verlangt,

Selbstdatenschutz

Argwohn riecht den Braten, ehe das Kalb geschlachtet ist. - Sprichwort

Da das Sammeln von personenbezogenen Daten für viele Serviceprovider von zentraler finanzieller Bedeutung ist, liegt es an dem einzelnen Benutzer, festzustellen wie viele persönliche Daten er bereit ist, dem Betreiber mitzuteilen bzw. zu veröffentlichen.

Ebenso ist es wichtig, dass der Betreiber die Anmeldung und das Ändern der persönliche Seite nur über HTTPS zugänglich macht und Passwörter nicht unverschlüsselt speichert oder per Email versendet. Dadurch wird

sichergestellt, dass selbst der Betreiber der Webseite den Account nicht ohne unverhältnismäßigem Aufwand benutzen kann und die Anmeldedaten nicht ohne Weiteres Dritten zugänglich machen kann

Generell ist es sinnvoll einem persönlichen Leitsatz zu folgen, was die Verbreitung der eigenen Daten betrifft, um sich die persönliche Würde und Privatsphäre zu erhalten. Sätze wie die hier gezeigten setzen einem Anwender ein Limit für übermittelte Daten.

"Telefonnummern nur an lokale Bekannte und Familie, Adresse nur mit triftigem Grund."

"Single-Use-Emailadressen für Single-Use-Webseiten"

> Manche Webseiten testet man nur einmal aus und verwendet sie nicht regelmäßig. Wenn die eigene Email-Adresse nicht kritisch für diesen Dienst ist, spricht nichts gegen das Anlegen einer temporären Adresse oder einer Weiterleitung, die später deaktiviert werden kann. So hat der Dienst keine Möglichkeit Emails an die primäre Email-Adresse zu senden wenn der Nutzer das nicht will.

Einteilung

Dennoch sollte man selbst eine Einteilung vornehmen. Ein Datensatz hat immer die Wertigkeit des gefährlichsten Dateneintrags. Ein Datensatz gilt als gefährlich, abhängig davon, wie einfach man damit zu kontaktieren ist und wie einfach er zu ändern ist. Ein Beispiel für eine Einteilung wäre:

allgemeine Angaben
die auf eine Vielzahl an Personen zutreffen und über die man nicht identifiziert werden kann. zB geteilte SPAM-Email-Adresse, Augenfarbe
Angaben unter Pseudonymen
Information kann keiner natürlichen Person zugeordnet werden, allerdings verweist das Pseudonym auf nur eine Person. Diese kann kontaktiert werden, aber das ist üblicherweise mit mehr Aufwand verbunden. Wenn die Person das Pseudonym ablegt ist ein Kontakt unmöglich. zB Forennick, zweckgebundene Email-Adresse, Nummer eines zweckgebundenen Wegwerf-Handys[8]
Angaben über die Realperson
Person kann anhand der Daten ausfindig gemacht werden, die Daten können nur mit Schwierigkeiten geändert werden. zB Name, Geburtsdatum, Adresse (auch teilweise), IP, KfZ-Kennzeichen, Telefonnummer
Angaben über sensible Bereiche der Realperson
Nicht nur sind solche Daten schwierig zu ändern, sondern lädt der Besitz solcher Daten zu Missbrauch ein. zB. Kreditkartennummer, Paypal-Passwort, Amazon-Passwort, PIN für EC-Karte, Kontonummer

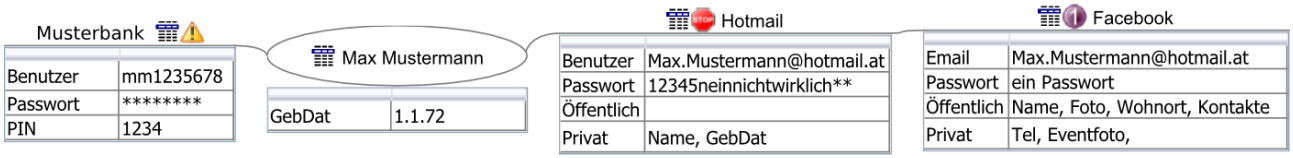
Wichtiger Punkt in der Anwendung ist, dass die verwendeten Dienste so wenig Einsicht wie möglich in die eigenen Daten haben, aber trotzdem noch Ihren Zweck erfüllen. Besonders Daten, die für den Benutzer schwierig zu ändern sind, sollten nicht achtlos weitergegeben werden.

8 billiges Mobiltelefon mit im Voraus bezahltem Guthaben

Datenbewußtsein

Um den Überblick zu behalten ist es manchmal sinnvoll, einen Mindmap[9] oder Liste der eigenen Online-Accounts zu erstellen. Neben Benutzernamen und (wenn die Liste an einem sicheren Ort aufbewahrt wird) Passwörtern kann auch festgehalten werden, über welche Daten der Betreiber des jeweiligen Dienstes verfügen kann und welche er veröffentlicht.

Dies muss nicht im Detail aufgezeichnet werden, Farbeinteilungen (wie zuvor beschrieben), Schlüsselwörter oder ähnliche Abstraktionen können hier ausreichen.



Der Prozess des Erstellung eines solchen Dokuments fördert das Bewusstsein über die mitgeteilten Daten und hilft, das Online-Bild der eigenen Person wahrzunehmen und in weiterer Folge auch an die eigenen Wünsche anzupassen.

Technische Methoden

Die folgenden Dienste werden häufig auch von Stalkern verwendet werden, um unerkannt zu bleiben, können aber auch effektiven technischen Schutz vor ihnen bieten

Anonymisierungsdienste

Es gibt ein breites Angebot von protokollspezifischen und protokoll-unabhängigen Anonymisierungsdiensten, die entweder nur Websurfen, Emails oder Chats oder den gesamten Internetverkehr über einen oder mehrere Server leiten, um die IP und damit die Herkunft und Ziel der versendeten und empfangenen Datenpakete verschleiern.

Protokollspezifische Dienste

Remailer verschleiern den Email-Verkehr.

> **Nym Remailer** verschleiert den Absender einer Email sowie andere Headerdaten, erlaubt jedoch eine Antwort des Empfängers über eine neue Email-Adresse, die nur ein (zB zufallsgeneriertes) Pseudonym, enthält. So kann der Name des Absenders nicht einfach über die Emailaddresse gefunden werden.
>
> **Cypherpunk Remailer** entfernen die Absenderadresse und machen dadurch das Antworten unmöglich. Zusätzlich benutzen die meisten Remailer dieser Art PGP-Verschlüsselung. Meist werden Nachrichten

9 Engl. Gedankenkarte; assoziationsgestützte Technik zum Erschließen bzw. visuellen Darstellen eines Themengebiets

über mehrere Remailer geleitet um den Eingangspunkt der Nachricht zu verschleiern.

Mixmaster Remailer verwenden ein eigenes Email-Format (benötigen daher spezielle Software zum Schreiben von Emails). Zusätzlich zu den Funktionen des Cypherpunk Remailer werden Nachrichten zwischengespeichert und zu zufälligen Zeitpunkten versendet. Große Nachrichten werden in kleinere Nachrichten (etwa 20kiB) zerlegt, kleinere Nachrichten werden aufgefüllt.

Mixminion ist noch in Entwicklung (Stand: Sept.2007). Es Erweitert das Konzept von Mixmaster Remailer um rotierende Verschlüsselung für die PGP Verschlüsselung zwischen den Knoten des versendenden Netzwerks.

Webproxies: Ein Proxy-Server leitet den Internetverkehr vom Anwender zum Webseitenbetreiber und verschleiert dadurch die IP Adresse des Anwenders. Manche Proxies können den Datenverkehr zwischenspeichern und sorgen damit für ein schnelleres Aufrufen der angeforderten Information.

Bouncer (zB für IRC[10] oder FTP[11]) arbeiten ähnlich einem Webproxy und leiten über einen entfernter Rechner die Anfragen an den Zielrechner weiter.

Protokollunabhängige Dienste

Ähnlich wie Webproxies können Anonymisierungsdienste über Protokolle wie **SOCKS**[12], **PPTP**[13] oder **OpenVPN**[14] einen gesicherten Tunnel zwischen dem Rechner des Anwenders und einem Proxy aufbauen. Durch einen solchen Tunnel wird der gesamte Internetverkehr geleitet, wobei die IP-Adresse des Anwenders wirkungsvoll verschleiert wird, egal welches Programm auf das Internet zugreift.

Eine Erweiterung hiervon ist ein P2P-Proxy-Netzwerk wie **JonDo**[15], **Tor**[16] oder **I2P**[17]. Jeder Anwender reicht Verbindungsdaten von anderen Anwendern weiter und fügt wenn notwendig eigene Daten hinzu. Die Datenpakete werden so mehrfach verschlüsselt ohne dass ein Knoten (außer Eingangs- und Ausgangspunkt) die Daten unverschlüsselt lesen kann. Rechtlich begibt man sich bei Benutzung eines solchen Netzwerks in eine Grauzone (oder macht sich gar strafbar), da man nicht erkennen kann welche Daten man weiterleitet. Möglicherweise leitet der eigene Knoten urheberrechtlich geschützte Werke, sensible Firmendaten oder Kinderpornografie weiter; ohne

10 Internet Relay Chat - ein rein textbasiertes Chat-System
11 File Transfer Protocol - Dateiübertragungsverfahren
12 SOCKet Secure - Datenweiterleitungsprotokoll
13 Point-to-Point Tunneling Protocol – Netzwerkprotokoll zum Aufbau von virtuellen privaten Netzwerken
14 quelloffenes Programm zum Aufbau eines Virtuellen Privaten Netzwerkes über eine verschlüsselte Verbindung
15 Anonymisierungsdienst
16 The Onion Router - Netzwerk zur Anonymisierung der Verbindungsdaten
17 Invisible Internet Project (dt. Projekt unsichtbares Internet) – Freie-Software-Projekt zur Schaffung eines anonymen bzw. pseudonymen Netzwerks

den Schlüssel für diese Datenpakete ist es unmöglich festzustellen, ob man sich der Beihilfe zu einer Straftat schuldig macht.

Geteilte Accounts

Trotz den Nutzungsbedingungen einer Webseite kann man Accounts für mehr als eine Person erstellen indem man die Zugangsdaten einem Bekannten mitteilt. So kann eine gemeinsame SPAM-Emailadresse oder ein Onlineshop-Profil für die ganze Familie erstellt werden. Dies erschwert das Erstellen eines Nutzerprofils erheblich, da der Nutzer scheinbar in unterschiedlichen Abständen andere Interessen und anderes Surfverhalten an den Tag legt. Der Nachteil ist, dass die Benutzer ihre Daten untereinander auf sehr intime Weise teilen.

Ob dieses Vorgehen sinnvoll ist, muss im einzelnen Fall erhoben werden und hängt stark von der Gestalt des verwendeten Dienstes ab.

Bearbeitung

Viele Webseitenanbieter, die persönliche Daten speichern, erlauben den Benutzern das Ändern ihrer Daten oder gar das Entfernen aller gespeicherten Daten. Vor einer Anmeldung ist dies definitiv zu prüfen oder falls das nicht möglich ist, ein Test-Account mit einer SPAM-Email-Adresse anzulegen und den Service zu testen bevor man ihn seriös verwenden möchte.

Manche Anbieter (zB. Facebook) speichern die Geschichte der Bearbeitungen mit und zeigen nur die aktuelle Version, was den Schutz durch Bearbeitung der eigenen Daten nur beschränkt wirksam macht.

Finanzielle Anonymisierung

Es existieren heute viele Möglichkeiten sicher und anonym im Internet einzukaufen. In österreichischen Trafiken, Postämtern und Supermärkten werden verschiedene Prepaid-Guthabenservices angeboten, die für eine Vielzahl von Diensten und Onlinekaufhäusern eingesetzt werden kann, wobei nur eine Email-Adresse zur Verwaltung von mehreren Karten registriert werden kann.

Banken und Finanzunternehmen bieten Kreditkarten auf Guthabenbasis an, die nicht immer an ein Bankkonto gebunden sein müssen (zB MasterCard RED bei Paylife). Diese sind, wenn das Guthaben gedeckt ist, weltweit einsetzbar, aber häufig mit höheren Kosten verbunden als gewöhnliche Kreditkarten.

Absichern gegen Tracking

Viele Webseitenanbieter haben es sich zur Aufgabe gemacht, Daten von Benutzern zu sammeln, egal ob sie sich auf deren eigenen Seiten oder auf Seiten von Drittanbietern bewegen. Dadurch lässt sich Interessensprofile der Anwender wesentlich einfacher und detaillierter erstellen.

Besonders Anbieter von Internetwerbung und sozialen Netzwerken haben großes Interesse an der Erstellung und Verwaltung von Interessensprofilen. In dem Zusammenhang wird in der Presse oft Google, Facebook und Amazon erwähnt.

2009 wurde eine Richtlinie der EU verabschiedet, die die Verwendung von Cookies[18] stark reglementieren sollte und so unfreiwillige Freigabe von Interessen eines Benutzers verhindern soll. Allerdings wurde die Richtlinie nicht von allen Mitgliedsstaaten umgesetzt und bleibt weiterhin ein kontroverses Thema.

Weit vor dem Versuch einer rechtlichen Lösung existierten jedoch technische Lösungen zum Erschweren bzw. Verhindern von Tracking.

Bei vielen Webbrowsern kann das Verhalten, wie mit Cookies verfahren werden soll, angepasst werden. Da Tracking besonders gut funktioniert, wenn Cookies über mehrere Browsersitzungen (also mehrere Tage oder Monate) bestehen bleiben, bietet sich das automatische Löschen von Cookies nach jeder Sitzung an, um einen Großteil der mit Tracking verbundenen Probleme zu verhindern.

Weiters verhindert das Blockieren von Javascript das Speichern von Cookies auf dem lokalen Rechner. Für versierte Anwender existiert eine breite Auswahl an Erweiterungen für den verwendeten Webbrowser, der bekannte Tracking-Skripte effektiv blockiert oder den Anwender auswählen lässt, welche Skripte er zulässt. Allerdings wird diese Vorgehensweise von vielen Anwendern nicht akzeptiert, da Javaskripte inzwischen Teil von fast jeder Webseite sind und selbstständiges Auswählen meist aufgrund des damit verbundenen Aufwands vernachlässigt wird.

Sichere Passwörter

> Geben Sie Ihre Passwörter nicht an Fremde weiter. Ändern Sie Ihre Passwörter regelmäßig. Passwörter sollten abwechslungsreich und unlogisch aus einem Mix aus Buchstaben und Zahlen bestehen.

Ein gutes Passwort[19]...

- ... ist mindestens 6 Zeichen lang, je länger desto besser.
- ... enthält Groß- und Kleinbuchstaben.
- ... enthält Ziffern, Sonder- und Satzzeichen.
- ... basiert nicht auf persönlicher Information.
- ... basiert nicht auf einem Wort aus dem Wörterbuch.

18 Kleine Dateien (meist zur Benutzeridentifikation) die auf dem Computer des Anwenders gespeichert werden. Erlaubt personenbezogene Werbung, aber ist auch für viele Webshop-Lösungen essentiell.

19 http://hitachi-id.com/password-manager/docs/choosing-good-passwords.html (abgerufen: Dez 2011) Choosing good passwords, Hitachi ID Systems, Inc. 2011

Um die Wahl eines sicheren Passworts zu Erleichtern wurden eine Vielzahl an Methoden entwickelt.

- Mehrere Wörter (min. 4) aus einem Wörterbuch, unlogisch verknüpft. (zB. "correct horse battery staple"[20] oder eingedeutscht "Pferdebatterienheftklammerkorrektheit"). Das Wort steht es in keinem Wörterbuch und ist alleine aufgrund seiner Länge schwer zu erraten, aber vergleichsweise leicht zu merken.
- Die Anfangs- oder Endbuchstaben jedes Wortes eines persönlichen Merksatzes. (z. B. "Ie90%dÄf7€!" gebildet aus den Zeichen von „Ich esse 90 % der Äpfel für 7 € !“)
- Passwortgeneratoren erzeugen rein zufällige Passwörter gewünschter Länge und reizen die Vielfalt des erlaubten Zeichensatzes aus. Allerdings sind solche Passwörter für viele Menschen schwer zu merken.

Mittels einer Kennwortverwaltung kann man das Aufschreiben und Abrufen von Passwörtern etwas sicherer gestalten. Allerdings sollte man sicherstellen, dass niemand unbefugt Zugriff auf die Passwortdatei hat und man ein gutes Master-Passwort wählt.

Moderne Browser bieten üblicherweise eine integrierte Passwortverwaltung, sowie die Möglichkeit Erweiterungen zu diesem Zweck nachträglich zu installieren.

Bei Verwendung von Onlinespeichern wie Lastpass ist zu bedenken, dass sie zwar bequemer sind, aber man abhängig vom Anbieter ist und die Passwortdatei permanent möglichen Angriffen ausgesetzt ist.

20 http://xkcd.com/936/ (abgerufen: Dez 11) Comic über Passwortstärke von Randall Munroe

Digitale Beziehungen

Passwörter teilen

In einer Telefonumfrage[21] wurde festgestellt, dass viele Jugendliche ihre Passwörter mit Freunden, Partnern oder Ihren Eltern teilen. Ob als Vertrauensbeweis, Absicherung bei Unfällen oder um Ablenkung vor einer wichtigen Prüfung zu vermeiden. Diese Praxis hat sowohl positive als negative Seiten. Sie erleichtern dem Passwortempfänger umfassende Möglichkeiten persönliche Daten einzusehen und auch sie zu manipulieren.

Sam Biddle[22] kommentierte das Teilen von Passwörtern in Liebesbeziehungen folgendermaßen:

Video-Portale: Wenn sich das Passwort von den anderen unterscheidet, ist teilen nicht nur unproblematisch sondern auch sinnvoll.

E-Mail: Schwerer Eingriff in die Privatsphäre, da der eigene Email-Account einerseits sensible Information enthält und andererseits auch von anderen Computern aufgerufen werden kann. Hier sollte die Sinnhaftigkeit definitiv hinterfragt werden, da der eigene Email-Account eine der wenigen Orte im Internet ist, wo noch ein gutes Maß an Privatsphäre herrscht.

Facebook: Schwerer Eingriff in die Privatsphäre, da auch Facebook private Nachrichten benutzt, die ähnlich schützenswert sind wie Emails.

Instant Messenger: Schwerer Eingriff in die Privatsphäre, da hier sehr leicht jemand anderer verkörpert werden kann. Niemand sollte auch nur nach diesen Zugangsdaten fragen.

Handy-PIN: Stellt kein gravierendes Risiko dar, obwohl hier kurzzeitig Einblick in die eigenen SMS-Nachrichten gewährt wird.

Computer: Bessere Variante ist sicher ein separater oder Gäste-Account, aber normalerweise ist das lokale Passwort (wenn es sich von den online verwendeten unterscheidet) kein gravierendes Sicherheitsrisiko.

Meine Interpretation dieser Vorschläge zeigt besonders den Unterschied zwischen lokalen und Online-Services. Lokale Passwörter (wie die Handy-PIN) können nur vor Ort verwendet werden, daher ist die Kenntnis dieser Information nutzlos ohne das dazugehörige Gerät. Video-Portale, der Autor nannte als Beispiel Netflix[23], können erst dann zur Gefahr werden, wenn zusätzliche Dienste massenhaft in Anspruch genommen werden, zB. Premiumkanäle oder Filmverleih. Üblicherweise wird aber eine Email an den Benutzer gesendet, um ihn von der Inanspruchnahme von Zusatzservices zu informieren.

21 http://pewinternet.org/Reports/2011/Teens-and-social-media/Part-3/Sharing-passwords.aspx
22 http://gizmodo.com/5870226/when-to-give-your-girlfriend-your-password
23 Ein US-amerikanischer Service der die Benutzer Serien und Filme legal und zu einem monatlichen Fixpreis empfangen lässt.

Kennenlernen

Kennenlernen im Internet ist heutzutage keine Seltenheit mehr. Sowohl Partneragenturen als auch Online-Kommunen haben diesen Vorgang wesentlich vereinfacht.

Leider existiert immer die Möglichkeit, dass die neue Bekanntschaft Signale missversteht und öfter Kontakt sucht als gewünscht.

Hintergrundcheck vor dem ersten Treffen

Das Kennenlernen neuer Personen ist ja prinzipiell nicht abzulehnen, unabhängig von Alter, Geschlecht oder sexuellen Orientierung. Jedoch sind einige Vorsichtsmaßnahmen zu treffen um auf der sicheren Seite zu sein.[24]

Folgende Methoden sind nicht ohne Fehler. Man findet möglicherweise viel Falschinformation bzw. Information die ein falsches Bild abgibt, ohne dass es die gesuchte Person etwas dafür kann. Es könnte sich zB. um eine gleichnamige Person handeln oder eine unbekannte Situation, die zu ungewollten Reaktionen führt.

Es liegt an der sozialen Kompetenz des Suchenden, konkrete Angaben zu finden. Gerade wenn der Gesuchte (wie es auch zu empfehlen ist) auf seine Online-Privatsphäre achtet, findet man wenig oder Falschinformation, allerdings kann man bei einer gründlichen Suche auf Warnungen vor dieser Person stoßen, falls er/sie anderen Benutzern bereits bekannt ist.

Öffentliche Einträge

Als grundlegenden Bild ergibt das Prüfen der bisherigen Einträge auf der Plattform, auf der der erste Kontakt stattfand (zB. welche Forenbeiträge wurden noch von der Person verfasst?). Des Weiteren gibt es viele öffentliche Einträge, in welchen Zusatzinformation ersichtlich ist. Viele (nicht alle) Personen sind im Telefonbuch vertreten, eine Suche auf Google, Facebook oder Twitter kann auch Einblicke in die soziale Umgebung und den geistigen Zustand der Person liefern.

Personenbezogene Suchmaschinen aggregieren Information aus vielfältigen Quellen und sind sehr anfällig für Fehler. Jedoch bieten sie manchmal eine Zusatzquelle zu öffentlichen Informationen, da sie Verknüpfungen zwischen verschiedenen Quellen berücksichtigen.

Verknüpfen der Ergebnisse

Die Ergebnisse einer Onlinesuche sind meist einzeln wenig aussagekräftig. Daher ist es sinnvoll, Querverweise zu finden, möglicherweise einen Mindmap zu erstellen.

24 http://lifehacker.com/5845900/how-to-use-the-internet-to-investigate-your-next-date-co+worker-or-new-friend-to-ensure-theyre-not-crazy

Sinnverwandte Einträge äußern sich durch ähnlichen Schreibstil und zeitliche Korrelation. Möglicherweise werden von der gesuchten Person mehrere Accounts verwendet. Wahrscheinlich ist es auch, dass sich hinter gleichen oder ähnlichen Spitznamen auf verschiedenen Netzwerken dieselbe Person verbirgt.

Der letzte Ausweg

Wenn andere Methoden versagen, kann es nützlich sein selbst Täuschung anzuwenden. Ein gefälschter Account mit einem attraktiven Foto ist manchmal hilfreich, um die Reaktionen der Person zu begutachten. Es ist jedoch zu bedenken, dass diese Täuschung nicht nur rechtlich fragwürdig ist und gegen übliche Nutzungsrichtlinien von sozialen Netzwerken verstößt, sondern auch ein falsches Bild der gesuchten Person abgeben kann, da sie in eine ungewohnte Situation versetzt wird.

Dennoch kann die Methode der Gegentäuschung eine Quelle für wichtige Informationen sein, wenn der Gesuchte auch nach gründlichem Nachforschen immer noch kein konsistentes Bild ergibt. Alternativ ist in so einem Fall ein Verschieben des Treffens auf später oder mehr Argwohn im Falle eines Treffens zu empfehlen.

Erstes Treffen

- erst wenn man mit ein Treffen einverstanden ist
- selbst fahren (kein No-Way-Back[25] Szenario riskieren)
- zentraler Ort mit viel Personenverkehr (zB ein Kaffeehaus)
- fixer Zeitrahmen (zB eine Stunde) danach u.U. ein ausgemachter Anruf von Freundin
- gemeinsame Freunde mitnehmen
- Vorsicht mit mitgeteilter Information (Finanzielle Infos, Wohnadresse,…)
- Andere wissen lassen, wo man zu finden ist (nicht nur die eigene Handynummer, sondern zB. auch die Festnetznummer des Ziels)

Das erste Treffen muss nicht romantischer Natur sein. Oft äußert sich der Wunsch, eine Online-Bekanntschaft persönlich zu vertiefen. Wichtig zu beachten ist, dass dieser Wunsch beidseitig ist. Wenn der andere nicht mit einem persönlichen Treffen einverstanden ist, sollte ein höfliches Ablehnen geäußert und akzeptiert werden.

Im Falle des beidseitigen Einverständnisses zu einem Treffen ist die Wahl des Treffpunkts und der Aktivität der nächste Schritt. Gerade beim ersten Treffen sollte die Wahl auf einen öffentlichen Ort mit viel Personenverkehr fallen, den alle selbst erreichen können (Das verhindert das Risiko eines No-Way-Back Szenarios.). Online-Partneragenturen raten meist zu einem kurzen ersten

25 Kein Weg zurück – keine Fluchtmöglichkeit bzw. keine Möglichkeit nach Hause zu kommen

Treffen, beispielsweise nur auf einen Kaffee[26], für einen kurzen persönlichen Eindruck. Zu lange erste Treffen sind meist wenig erfolgreich, also ist ein begrenzter Zeitrahmen durchaus sinnvoll.

Falls gemeinsame Bekannte existieren, können diese Sie bei einem ersten Treffen begleiten und auch ein Gesprächsthema bieten. Online-Partneragenturen raten von einer ausgedehnten Selbstdarstellung beim ersten Treffen ab, was nicht nur soziale Gründe hat sondern auch Schutz davor bietet, zu viel eigene Information preiszugeben. Auf jeden Fall sollten heikle Daten wie die Wohnadresse oder finanzielle Informationen vorerst tabu sein.

Selbst wenn keine gemeinsamen Bekannte existieren, sollte das Treffen keineswegs geheim bleiben. Andere wissen zu lassen, wo man zu finden sind, ist kein Vertrauensbruch, eher eine Vorsichtsmaßnahme. Die eigene Handynummer reicht in diesem Fall nicht aus, die Festnetznummer oder Adresse des Treffpunkts ist aufgrund der Rückverfolgbarkeit eine wesentlich bessere Wahl.[27]

Nach oder während dem Treffen kann auch eine Rückmeldung an die Vertrauensperson erfolgen.

26 http://www.elitepartner.de/magazin/sieben-fallen-beim-ersten-date-2.html
27 http://friendship.about.com/od/Meeting-New-Friends/tp/Safety-Tips-When-Meeting-New-Friends.htm

Trennung

Die Trennung einer intimen Beziehung bzw. Scheidung einer Ehe ist oftmals Anlass für Stalking- und Cyberstalking.

Trennungsphasen

Gerade weil die emotionalen Phasen der Trennung bei den einzelnen Partnern nicht synchron verlaufen, kann es hier zu Konflikten kommen.[28]

1. **Nicht-Wahrhaben-Wollen und Verleugnen**

   Sie glauben an einen bösen Traum, hoffen darauf, dass alles wieder gut werden wird. Sie bemühen sich, den Partner umzustimmen. Sie würden fast alles tun, um den Partner wiederzubekommen. Sie verschließen die Augen vor der Trennung und tun so, als sei nichts geschehen.

2. **Aufbrechende Gefühle**

   Sie werden überrollt von Ihren Gefühlen, sind verzweifelt, voller Angst, plagen sich mit Selbstzweifeln, Eifersucht, Wut und Hass. Sie können nicht gut schlafen, essen nicht oder zu viel, sind voller Unruhe, haben Verstopfung, Kopf- oder Magenschmerzen, Herzrasen, usw. Sie grübeln "warum nur?" und denken ununterbrochen an den Partner. Sie ziehen sich von Freunden zurück oder flüchten sich in Aktivitäten. Nicht wenige Verlassene sind anfänglich depressiv und nichts und niemand kann sie trösten und ihnen den Schmerz und die Einsamkeit nehmen.

3. **Neuorientierung**

   So langsam sehen Sie Land. Sie können sich wieder alleine beschäftigen, Ihre Wut und die Verzweiflung angesichts der Trennung nehmen ab. Sie können loslassen, sich wieder auf das Heute und Morgen und Ihr Leben konzentrieren.

4. **Neues Gleichgewicht**

   Sie verspüren wieder Selbstvertrauen, verstehen, weshalb die Partnerschaft zerbrach und es zur Trennung kam. Sie haben wieder eine Zukunfts-perspektive.

Abstand gewinnen

Dr. Doris Wolf schlägt in ihren Empfehlungen unter Anderem vor, Kontakt zu seinem ehemaligen Partner zu meiden. Doch gerade in der vernetzten Welt der sozialen Netzwerke ist das ein schwieriger Vorgang. Immer wieder kann man unbeabsichtigt auf Neuigkeiten im Leben des ehemaligen Partners stoßen, die emotional verstörend sind und der Neuorientierung hinderlich sind.

Das sollte das Trennungs-Drama[29] minimieren, das sich auf Onlineplattformen leicht hochschaukeln kann und unvorhersehbare Nebenwirkungen haben kann. Auch sollte nach Möglichkeit Nachstellen durch Dritte minimiert werden.[30] [31]

28 Dr. Doris Wolf - Bewältigung einer Trennung http://www.palverlag.de/trennungsschmerz-hilfe.html (Abgerufen: Dez 2011)
29 Überdramatisierung bei Konversationen im Internet
30 Alan Henry - http://lifehacker.com/5830264/how-to-banish-your-ex-from-of-your-digital-life
31 Sam Biddle - http://gizmodo.com/5779809/how-to-survive-the-modern-day-breakup?

Facebook

Verstecken des Eintragungen vom Ex-Partner (verhindert nur das Auftauchen von Updates die unter Umständen verletzend sein können, behindert aber keine anderen Einschränkungen für den Ex-Partner)“Freundschaft beenden” funktioniert ohne Benachrichtigung des Ex-Partners, könnte aber als höchst beleidigend angesehen werden“Beziehungsstatus ändern” sind gut sichtbare Einträge in Facebook, können aber in den Einstellungen für Privatsphäre für den Freundeskreis versteckt werden, wenn auch nur um die Änderung durchzuführen und sich eine Menge peinlicher Kommentare zu ersparen … und nicht mögliche Dritte vom Nachstellen (da man ja wieder Single ist) zu ermutigen.Problem der gemeinsamen Fotos bezieht Dritte (den Uploader) mit ein. Untagging funktioniert gut im Einzelfall aber wenn viele Fotos vorhanden sind, existiert derzeit kein einfacher schneller Weg, diese zu entfernen.

Twitter

Unfollow und Block könnte Trennungsdrama verschärfen und Dritte auf die emotional heikle Situation aufmerksam machen. Manche Twitter-Clients können die Tweets eines bestimmten Benutzers ausblenden, ähnliches gilt auch für Foursquare.

Google+

Einen “stillen” Kreis (also ein Kreis von dem man keine Nachrichten erhält) erstellen und den Ex-Partner hinzufügen.

Email

Anlegen eines Filters mit der Email-Adresse des Ex-Partners. Mails sollten nicht gelöscht werden, aber in einen durchsuchbaren Ordner verschoben werden, damit man nicht ständig erinnert wird.

Instant Messaging[32]

Den Ex-Partner zu blocken führt bei den meisten IM-Programmen dazu, daß der Ex-Partner keine Nachrichten mehr an den eigenen Account schicken kann und auch nicht mehr sieht wenn man online ist.Falls das IM Netzwerk das zulässt, sollte der Onlinestatus nur den eigenen Kontakten zugänglich sein. Somit hat man mehr Kontrolle über die eigene Sichtbarkeit. Erweiterungen zum Schutz der Privatsphäre (zB. Pidgin Privacy Please[33]) ermöglichen noch genauere Verwaltung, zB. verstecken von erhaltenen Nachrichten des Ex-Partners, sowie automatische Antworten.

32 ICQ, MSN, Google Talk, AiM, Skype …
33 Erweiterung des Sofortnachrichtenprogramms Pidgin

Telefon/SMS

Im deuschsprachigen Raum ist das Blockieren von Telefonanrufen durch den Anbieter nicht üblich. Viele Smartphones verfügen allerdings über Apps die Anrufe von bestimmten Nummern und auch SMS blockieren können.

Bei Problemen

Da ein Partner sich leicht Zugang zu PC und anderen internetfähigen Geräten verschaffen kann, ist es wichtig hier Vorkehrungen zu treffen[34].

Unter Umständen kann es zu verdächtigen Situationen kommen, wie eine Flut an unerwünschten (Werbe-)Mails oder einer ungewissen Abbuchung am Konto oder per Kreditkarte. Hier sollte schnell gehandelt werden, da schnelles gewissenhaftes Agieren für viele Stalker abschreckend wirkt.

Eigene Systeme (PC,Laptop,Smartphone) sauber halten!

- regelmäßige Datensicherung
  - Updates von Betriebssystem und Antivirenprogramm einspielen
  - Verwendung von sicherer Software, gerade bei vertraulichen Kommunikation (zB. mit Polizei und Anwalt) auf Verschlüsselung achten (zB mittels PGP[6])
- Smartphones
  - auf Spionagesoftware prüfen bzw. prüfen lassen (SMS, Email, Kalenderdaten können von kleinen Serviceprogrammen leicht weitergesendet werden)
  - sind besonders anfällig für Spionageangriffe. Hier sollte besondere Vorsicht gelten und bei Unsicherheit eine Neuinstallation vorgenommen werden. Verwendete Nutzerdaten (zB Email-Passwort) sollten vorher sichergestellt werden.

eigene Online-Accounts

- Anmeldedaten auf Änderung prüfen
  - Email-Accounts
  - Soziale Netzwerke und damit verknüpfte Dienste
  - Onlinebanking (auch Paypal o.Ä.)
  - Onlineshops (auch Account-Daten von AppStores)
- Passwörter ändern (sodass auch der Ex-Freund sie nicht erraten kann)
  - auch Sicherheitsfragen ändern (hier kann ein Ex-Partner möglicherweise leicht einbrechen)
  - Vorkehrungen bei Verwendung eines Passwortmanagers
    - Ändern des Hauptkennworts
    - Ändern der einzelnen Passwörter
    - u.U. Löschen und Neuerstellung eines anderen Accounts.

34 Alexis A. Moore - http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm

- Email-Accounts auf unerwünschte Weiterleitung prüfen
- u.U. Email-Adresse ändern

fremde Online-Accounts unter dem eigenen Namen

- über (Personen-)Suchmaschinen prüfen wo der eigene Name aufscheint
- Beliebte Angriffsziele: Soziale Netzwerke wie Facebook, aber auch Netzwerke zum wiederfinden alter Schulfreunde[35]
- prüfen ob tatsächlich Identitätsmissbrauch vorliegt (eigenes Foto, Kontaktdaten), wenn ja:
  - Seitenbetreiber kontaktieren
  - Polizei einschalten

Finanzsysteme

- neue Kreditkartennummer
- Wechsel der Bankomat-PIN
- e-Banking Passwort ändern
- Passwort für Online-Bezahlsysteme ändern (gilt für Paypal/Google Checkout/ Paybox aber auch für alle Webseiten die Finanzinformationen speichern wie Amazon, PS-Network, ...)
- Bankmitarbeiter darauf hinweisen dass der Ex-Partner keine Befugnisse zum Ändern bzw. Einsicht (mehr) hat
  - Wenn der Ex bei der Bank arbeitet, sicherheitshalber Bank wechseln

35 z.B. www.klassentreffen.at

Abschließende Worte

Die neuen Medien sind ein schwer zu überblickendes Thema, aber man kann annehmen, dass das letzte Wort zum Thema „Cyberstalking“ noch nicht gesprochen ist.

Ständig werden neue Formen der digitalen Kommunikation gefunden und in Software umgesetzt. Jede neue Entwicklung bietet Raum für Missbrauch und unethisches Handeln, jedoch bieten sie dem Kundigen auch mehr Optionen für Sicherheit und Zufriedenheit. Neben technischem Verständnis sind auch zwischenmenschliche Fähigkeiten für ein besseres Miteinander unerlässlich.

Das Rechtssystem hilft hier nur zu einem gewissen Grad. Grobe Vergehen und Fehler im Vorgehen der Täter sind oft erst Anlass für Anzeige und rechtliche Verfolgung. Obwohl die Zahl der gemeldeten Fälle von Computerkriminalität steigt, bleiben viele Fälle unerkannt und damit unbearbeitet oder werden zu spät erkannt um erfolgreiche Ermittlungen durchzuführen.

Auch wenn die Ermittlungsmethoden der Polizei gestärkt werden, ist das kein Grund, sinnvolle Maßnahmen für seine persönliche Sicherheit außer Acht zu lassen. Dies wird mögliche Attacken nicht verhindern, aber um ein gewisses Maß unwahrscheinlicher werden lassen, sowie Angriffe, sollten sie passieren, sichtbar machen.

Quellen

- Cornelia Belik – Cyber stalking Ergebnisse einer Onlinebefragung (Books on Demand GmbH 2007, ISBN 978-383-700-849-4)
- WHO@ cumulative statistics http://www.haltabuse.org/resources/stats/index.shtml (abgerufen: Jänner 2012)
- Choosing good passwords, Hitachi ID Systems, Inc. 2011 http://hitachi-id.com/password-manager/docs/choosing-good-passwords.html (abgerufen: Dez 2011)
- Comic über Passwortstärke von Randall Munroe http://xkcd.com/936/ (Abgerufen: Dez 2011)
- Amanda Lenhart, Mary Madden, Aaron Smith, Kristen Purcell, Kathryn Zickuhr, Lee Rainie - One in three online teens has shared a password with a friend or significant other. (Blog vom 9. Nov. 2011) http://pewinternet.org/Reports/2011/Teens-and-social-media/Part-3/Sharing-passwords.aspx (Abgerufen: Nov 2011)
- Sam Biddle - When to Give Your Girlfriend Your Password http://gizmodo.com/5870226/when-to-give-your-girlfriend-your-password (Abgerufen: Nov 2011)
- Adam Dachis - How to Use the Internet to Investigate Your Next Date, Coworker, or New Friend (Without Being Creepy) http://lifehacker.com/5845900/how-to-use-the-internet-to-investigate-your-next-date-co+worker-or-new-friend-toensure-theyre-not-crazy (Abgerufen: Okt 2011)
- Annette Riestenpatt - Vorsicht Falle: Sieben Fallen beim ersten Date http://www.elitepartner.de/magazin/sieben-fallen-beim-ersten-date-2.html (Nov 2011)
- http://friendship.about.com/od/Meeting-New-Friends/tp/Safety-Tips-When-Meeting-New-Friends.htm (Abgerufen: Nov. 2011)
- Dr. Doris Wolf - Bewältigung einer Trennung http://www.palverlag.de/trennungsschmerz-hilfe.html (Abgerufen: Dez 2011)
- Alan Henry – How to banish your Ex from your digital life http://lifehacker.com/5830264/how-to-banish-your-ex-from-of-your-digital-life (Abgerufen Okt 2011)
- Sam Biddle – How to survive the modern breakup? http://gizmodo.com/5779809/how-to-survive-the-modern-day-breakup? (Abgerufen: Jan 2012)
- Alexis A. Moore - 12 Tips To Protect Yourself From Cyberstalking http://womensissues.about.com/od/violenceagainstwomen/a/CyberPrevention.htm (Abgerufen: Nov 2011)