DEUTSCHER PRÄVENTIONSTAG

„Internetkriminalität 2008 - Gefahren-Maßnahmen-Anlaufstellen“

von

Rolf Grimmer

Dokument aus der Internetdokumentation
des Deutschen Präventionstages www.praeventionstag.de
Herausgegeben von Hans-Jürgen Kerner und Erich Marks im Auftrag der
Deutschen Stiftung für Verbrechensverhütung und Straffälligenhilfe (DVS)

Zur Zitation:
Rolf Grimmer: Internetkriminalität 2008 - Gefahren-Maßnahmen-Anlaufstellen, in: Kerner, Hans-Jürgen u. Marks, Erich (Hrsg.), Internetdokumentation des Deutschen Präventionstages. Hannover 2008, www.praeventionstag.de/Dokumentation.cms/438

INTERNETKRIMINALITÄT

Gefahren – Schutzmaßnahmen - Anlaufstellen

1. Einleitung

Ziel des Vortrages ist es, Ihnen einen Überblick über die Kriminalität im Internet zu geben.

Der Vortrag ist dazu in vier Bereiche gegliedert:

Das Internet

Als Einstieg erhalten allgemeine Informationen und einen Blick auf die Besonderheiten.

Die Gefahren

Hier werden wir die Gefahren und Risiken genauer betrachten.

Die Schutzmaßnahmen

Wie kann man die Risiken minimieren? Was kann man präventiv tun?

Was kann man als User persönlich tun?

Anlaufstellen

Wo kann man sich beraten lassen oder wo kann man Verdachtsfälle melden?

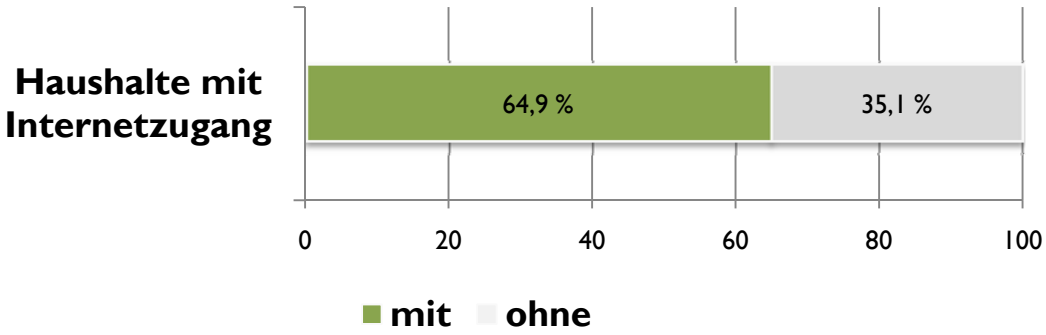
Was kann ich als Opfer tun?

Danach haben wir Zeit für Fragen oder eine kurze Diskussion.

Anmerkungen sind grün gekennzeichnet.

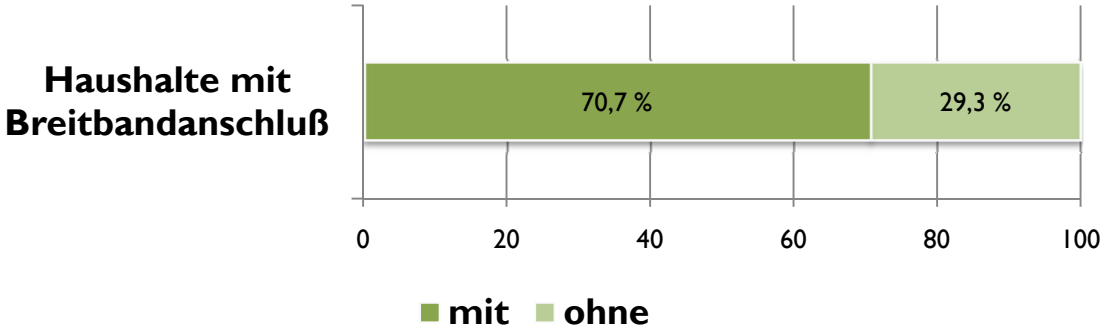
2. Das Internet

Beginnen wir mit dem Internet. Es ist schon längst weit mehr als nur bunte Webseiten mit blinkenden Grafiken. Immer mehr Menschen nutzen die Möglichkeiten des Internets. Der Großteil ruft Informationen ab oder kommuniziert per E-Mail.
Sehen wir uns dazu ein paar Zahlen an.



Zurzeit verfügen in Deutschland 65 % der Haushalte über einen Internetzugang. Das entspricht ca. 26 Millionen Haushalte (2006: 39.766.000)[1].

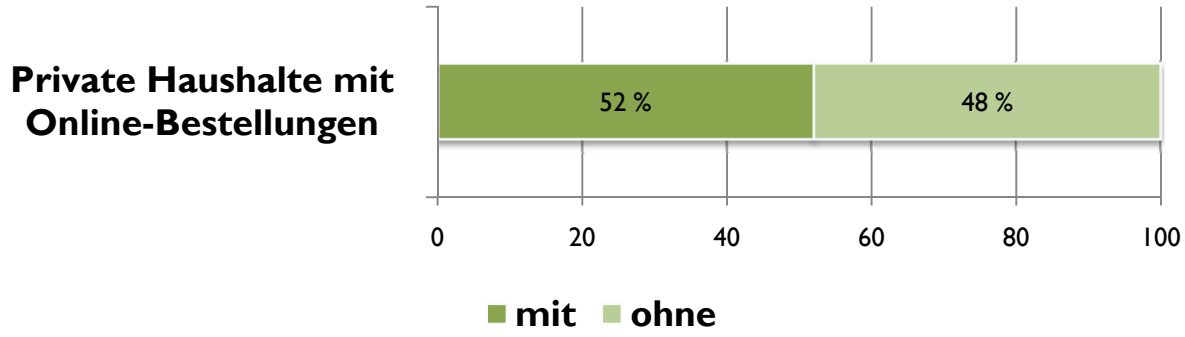
Über 70 % davon verfügen sogar über einen Breitbandanschluss. Den restlichen 30 % steht ISDN oder eine recht langsame analoge Verbindung zur Verfügung.



Wobei die Versorgungsdichte von DSL-Anschlüssen nicht 100% beträgt. Nicht jeder, der einen schnellen Zugang wünscht, kann diesen auch erhalten. Es gibt noch immer viele Ortschaften, die keine Möglichkeit haben einen Breitbandanschluss zu nutzen. Beispiel: [2].

[1] Statistisches Bundesamt, Die Bundesländer 2008, https://www-ec.destatis.de/csp/shop/sfg/bpm.html.cms.cBroker.cls?cmspath=struktur,vollanzeige.csp&ID=1021999
[2] 29.05.2008: Finning, nur 40 % haben Breitband. http://www.augsburger-allgemeine.de/Home/Lokales/Landsberg/Uebersicht/Artikel,-DSL-Telekom-ruestet-nach-_arid,1233878_regid,2_puid,2_pageid,4500.html

52 % der Haushalte mit Internetanschluss haben schon Bestellungen / Buchungen online durchgeführt[3]. Das entspricht auch ungefähr der Anzahl Menschen, die das Internet für Behördenkontakte nutzen, nämlich 27 Millionen. Es nehmen 43% der Bevölkerung im Alter von 16 bis 74 Jahren am E-Goverment teil[4].



Weitere Zahlen

- Da pro Haushalt durchschnittlich 2,08 Personen leben, haben somit über 50 Millionen Personen in Deutschland Zugang zum Internet.
- 95 Prozent aller Firmen verfügen über Web-Zugang[5].
- 15 Millionen Deutsche buchen ihren Urlaub online[6].
- Fünf von sechs Teenagern sind aktive Internet-Nutzer[7].
- Jeder zehnte Blumenstrauß wird im Web gekauft.
  Rund 300 Millionen Euro Online-Umsatz wird mit Schnittblumenverkäufen jährlich realisiert[8].

Rund ein Fünftel aller Steuererklärungen werden über das Internet übermittelt[9].

Doch das Internet bietet schon jetzt weit mehr als Informationen und Schnittblumen. Ihnen muss bewusst werden, dass immer mehr Aufgaben/Dienstleistungen/Lebensbereiche aus dem realen Leben auf das Medium Internet übertragen werden.

Wir sind zwar noch weit entfernt von einer „virtuellen Welt“, doch schon heute ist es möglich nur mit einem Computer und einer Internetverbindung zu „überleben“. Man kann am Rechner arbeiten (Geld verdienen), einkaufen, rechtskräftige Verträge abschließen, Behördengänge erledigen. Alles ohne das Haus zu verlassen. Auch den Müll können sie sich am Ende des Tages abholen lassen. Dies

[3] Statistisches Bundesamt Deutschland: http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Navigation/Statistiken/Wirtschaftsrechnungen ZeitbudgetsPrivateHaushalteInfoGesellschaft/PrivateHaushalteInfoGesellschaft.psml
[4] http://www.destatis.de/jetspeed/portal/cms/Sites/destatis/Internet/DE/Presse/pm/zdw/2008/PD08__008__p002,templateId=renderPrint.psml
[5] BITCOM: http://www.bitkom.de/de/presse/8477_51454.aspx
[6] BITCOM: http://www.bitkom.de/de/presse/8477_51068.aspx
[7] BITCOM: http://www.bitkom.de/de/presse/8477_50560.aspx
[8] BITCOM: http://www.bitkom.de/de/presse/8477_52109.aspx
[9] BITCOM: http://www.bitkom.de/de/presse/8477_52285.aspx

geschieht alles ausschließlich durch die Kommunikation über das Internet. Dazu braucht man nur einen Computer oder Laptop.

Hört sich doch alles gut an! Wir erreichen immer mehr Menschen, entwickeln immer mehr Innovationen. Doch wo sind da die Gefahren? Sie sind doch zu Hause! Sicher! Sicher?

Nein! Denn unser „reales Leben" enthält eine Menge von Risiken und je mehr sinnvolle Dienstleistungen und Mehrwerte im Internet angeboten werden, je mehr Personen aktiv am Internet teilnehmen, so werden ebenfalls die damit verbunden klassischen kriminellen Handlungen aufs Internet verlagert. Das bedeutet: Was Ihnen im normalen Leben passieren kann, kann Ihnen auch im Internet geschehen.

Nur ist dort alles etwas schlimmer. Denn das Internet hat für Sie ein paar Besonderheiten parat.
Ich will Ihnen keine Angst machen. Nur sensibilisieren.

Was macht das Internet besonders und warum Gefährdungspotential höher ist

Das Internet kennt keine Entfernungen

Der Aufenthaltsort des Täters ist ebenso beliebig wie der Ort, wo Schaden verursacht wird. Täter und Opfer können tausende Kilometer von einander entfernt sein, aber im Internet ist es nur ein Klick. Bei ca. 1.4 Milliarden aktiven Usern[10] im Internet, wird jedem klar, dass man nicht nur von Kriminellen aus Deutschland bedroht wird. In dem eigenen Haus. Man ist im eigenen Haus dem Risiko ausgesetzt, Opfer eines Täters aus dem Ausland zu werden. Dies ist einer der Gründe, warum die Strafverfolgung schwieriger ist. Zudem kann bei einem einzigen Fall eine Vielzahl von Ländern verwickelt sein.

Angriffe sind reproduzierbar. Mit einem Klick

Es ist eine Charaktereigenschaft der digitalen Welt. Daten, Programme, Abläufe, alles kann man 1:1 kopieren. Ohne Verluste. Die Kopie ist das Original. Es gibt keinen Unterschied.
Im Internet kursiert zu Hauf kostenlose Software, Skripte oder Virenbaukästen mit denen ohne Vorkenntnisse Angriffe gestartet werden können. Inklusive der strafrechtlichen Folgen. Was häufig auch von den „Scriptkiddies" nicht beachtet wird. Was kann so schlimm sein, eine paar E-Mails zu versenden?

Nun. Früher wäre es vielleicht einem aufgefallen, wenn man 30.000 Briefe kuvertiert und per Post versendet. Man würde sich überlegen, welche Nachricht man versendet. In der digitalen Welt hingegen, scheint es egal zu sein.

[10] http://www.internetworldstats.com/stats.htm

Angriffe sind kostengünstig

Die 30.000 Briefe wollen ja nicht nur zur Post getragen werden, auch die Frankierung kostet Geld. In unserer „perfekten“ Welt, dem Internet, kostet es nichts. Was immer Kriminelle vorhaben, es reicht ein Laptop, eine Internetverbindung und das Wissen.

Eigentlich nur ein Laptop. Es gibt noch genügend ungeschützte W-LANS. Dort erhält man eine kostenlose Internetverbindung. Das notwendige Wissen und Werkzeuge für die Begehung einer Straftat findet man auch kostenlos im Internet.

Angriffe sind unter Umständen vollständig anonym

Ein krasser Unterschied, wenn man es mit der klassischen Strafverfolgung vergleicht. Und eine noch nicht zufrieden stellend gelöste Problematik. Beispiel: In den USA wird ein offenes W-LAN genutzt oder sich in ein unsicheres „gehackt“. Von dort aus wird ein Rechner in Deutschland mit Schadcode infiziert und dazu gebracht massenweise E-Mails zu versenden.

Wer haftet? Auf jeden Fall nicht der Verursacher. Der wird tatsächlich anonym bleiben. Abgesehen von dem derzeit hohem Aufwand den Namen des Betreibers vom W-LAN aus den USA herauszubekommen. Der Betreiber war es nicht und wird es natürlich auch vehement abstreiten. Trotzdem die Spur direkt zu ihm führt.

Im Landgericht Hamburg lautete das Urteil vom 27. Juni 2006 (Az. 308 O 407/06): Ob die Rechtsverletzungen selbst begangen wurden oder ob sie aufgrund einer Nutzung des ungeschützten WLAN durch Dritte erfolgt ist, ist unerheblich. Die Beklagten hätten für diese Rechtsverletzung jedenfalls nach den Grundsätzen der Störerhaftung einzustehen.

Eine Mitverantwortung also. Ist schon hart, wenn man darüber nachdenkt. Accesspoints werden fast immer ungesichert ausgeliefert, sie sollen per Plug-and-Play funktionieren. Ist jedem zu zumuten ein W-LAN korrekt abzusichern? Wäre er nach diesem Urteil nicht sogar dazu verpflichtet? Und wenn ja, warum wird er nicht darauf aufmerksam gemacht?

Und selbst wenn er es schützt, aber jemand sich trotzdem einhackt und den Computer missbraucht. Wer wird haften? Fakt ist, der tatsächliche Verursacher bleibt im Hintergrund.

Kommt so etwas häufiger vor? Ich will es mal so sagen: Dieses Vorgehen hat schon einen Namen: „Wardriving“. Wardriving bedeutet das systematische Suchen nach W-LANS mit Hilfe eines Fahrzeuges. Es gibt auch „Drive-by-Hacking“ oder „Drive-by-Pharming“ und weitere, wobei es immer darum geht, einen fremden Internetanschluss für eigene Zwecke zu missbrauchen.
Und dabei natürlich unentdeckt zu bleiben.

Das Internet ist flexibel, hinterhältig, geduldig

Es ist schwierig, unseriöse „Subjekte“ zu erkennen. Männer geben sich als Frauen aus, Alte als Junge, gerade gegründete Firmen präsentieren sich als alt eingesessen mit großem Kundenkreis.

Wieder ein Vergleich zu unserer „physischen Realität“. Wenn Sie ein neues Geschäft sehen und es betreten, dann wissen Sie, wo sie sich aufhalten. Auf der Ihnen bekannten Straße haben Sie einen Stopp gemacht und das Geschäft betreten. Sie würden sich nicht fragen, ob Sie sich noch im gleichen Land befinden. Sie würden sich auch nicht fragen, ob die Ware, die Ihnen angeboten wird überhaupt existiert.

Im Internet hingegen sind Texte und Grafiken für eine „visuelle Bewertung“ wertlos. Denn in der digitalen Welt können Sie auf „Online-Shops“ stoßen, deren Inhalte von seriösen Webseiten zum Teil oder vollständig kopiert wurden. Vom Aussehen her sind sie nicht von einem echten Shop zu unterscheiden. Es müssen keine Geschäftsräume gemietet werden, es steht kein Personal an der Kasse. Es wird auch kein Lager für die Ware benötigt, es reichen Fotos davon.

Das Internet ist geduldiger als Papier.

3. Gefahren

Klassische Straftaten (Internet ist nur Mittel zum Zweck):

- Illegale Inhalte
- Betrug
- Beleidigung
- Erpressung
- Fälschung
- Urheberrechtsverletzung und verwandter Schutzrechte

Gefahren, die sich direkt gegen das „Internet“ richten

Vertraulichkeit

Die Vertraulichkeit („Secrecy“ oder auch „Privacy“), wird gewahrt, wenn eine Information nicht durch unberechtigte Dritte kompromittiert wird. Das bedeutet, dass der Inhalt oder sogar die Existenz der Information nicht unberechtigten Dritten zur Kenntnis gelangt.

Integrität

Integrität bedeutet die Sicherstellung der Vollständigkeit und Korrektheit von Informationen, aber auch die korrekte Funktionsweise von Systemen, die Systemintegrität. Nur festgelegte Gruppen können definierte Informationen modifizieren oder löschen. Dies gilt für alle Daten die verarbeitet, übertragen oder gespeichert werden.

Aktuelles Beispiel: China-Website des Roten Kreuzes wurde gehackt.
Nach von der chinesischen Sicherheitsbehörde (Ministry of Public Security) bestätigten Informationen haben sich Hacker Zugriff auf einen Bereich der chinesischen Web-Seite des Roten Kreuzes verschafft, der auf die Konten für die eingehenden Spenden verweist[11].

Verfügbarkeit

Alle Informationen und die damit verbundenen Systeme müssen jederzeit verfügbar und in der geforderten Qualität bereit stehen. Dies betrifft insbesondere die Hardware und Software, und natürlich auch die archivierte Daten.

Authentizität / Identitätsdiebstahl

Authentizität bedeutet die Sicherstellung der Echtheit der behaupteten Identität bzw. der Echtheit von Informationen.

[11] ZDNET, 19.Mai 2008: http://www.zdnet.de/security/news/0,39029460,39191038,00.htm

Jeder achte Deutsche telefoniert übers Internet.12 Dave Gladwin, Mitarbeiter des VoIP-Anbieters Newport Networks, berichtet gleichzeitig, dass gestohlene Zugangsdaten von VoIP-Usern mittlerweile für 17 Dollar pro Account am Online-Schwarzmarkt zu haben seien. Zwar befinde sich dieser Zweig der Internet-Kriminalität noch am Anfang, wachse aber mit der zunehmenden Bedeutung von VoIP[13].

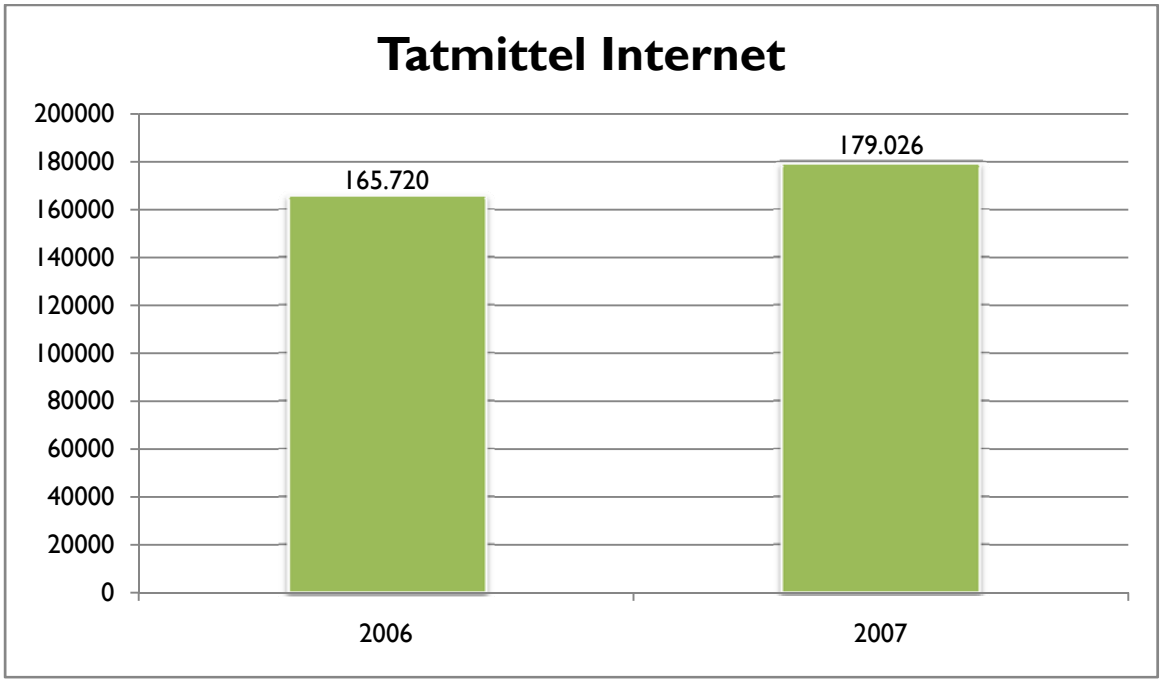
Ziel sind alle Teilnehmer am Internet

Privatpersonen, Unternehmen, Behörden / Regierungen

[12] BITCOM, 16. April 2008: http://www.bitkom.de/de/presse/39858_51603.aspx
[13] BBC-News, 14. Mai 2008: http://news.bbc.co.uk/2/hi/technology/7398676.stm

Straftaten mit Tatmittel Internet

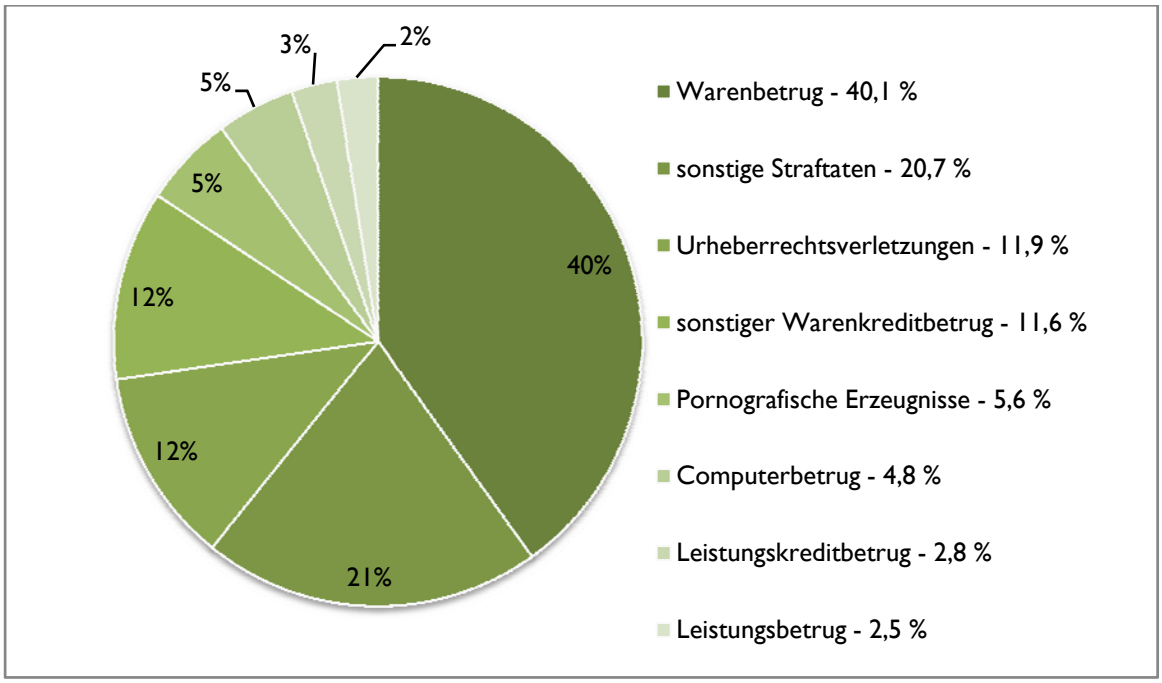
Seit 2006 wird in 15 Bundesländern die Sonderkennung „Tatmittel Internet“ verwendet.



Kein großer Unterschied. „Nur“ 8,0 % Steigerung im Vergleich zum Vorjahr.

Quelle: Polizeiliche Kriminalstatistik 2007[14]

Betrugsarten mit dem Tatmittel Internet



Quelle: Polizeiliche Kriminalstatistik 2007[15]

[14] BKA: http://www.bka.de/pks/pks2007/pks2007_imk_kurzbericht.pdf
[15] BKA: http://www.bka.de/pks/pks2007/pks2007_imk_kurzbericht.pdf

Warenbetrug
Ein Verkäufer liefert nach Erhalt der Zahlung die Ware in minderwertiger Qualität, gar nicht oder behauptet wahrheitswidrig die durchgeführte Lieferung.

Sonstige Straftagen
Zugriff auf Rechnersysteme, das Abhören von Daten, Störung von Computersystemen und der Missbrauch von Geräten und Programmen.

Urheberrechtsverletzungen
Bei Filmen, Musikstücken, Bücher, Computerprogrammen, Datenbanken, etc. Copyrightverletzung

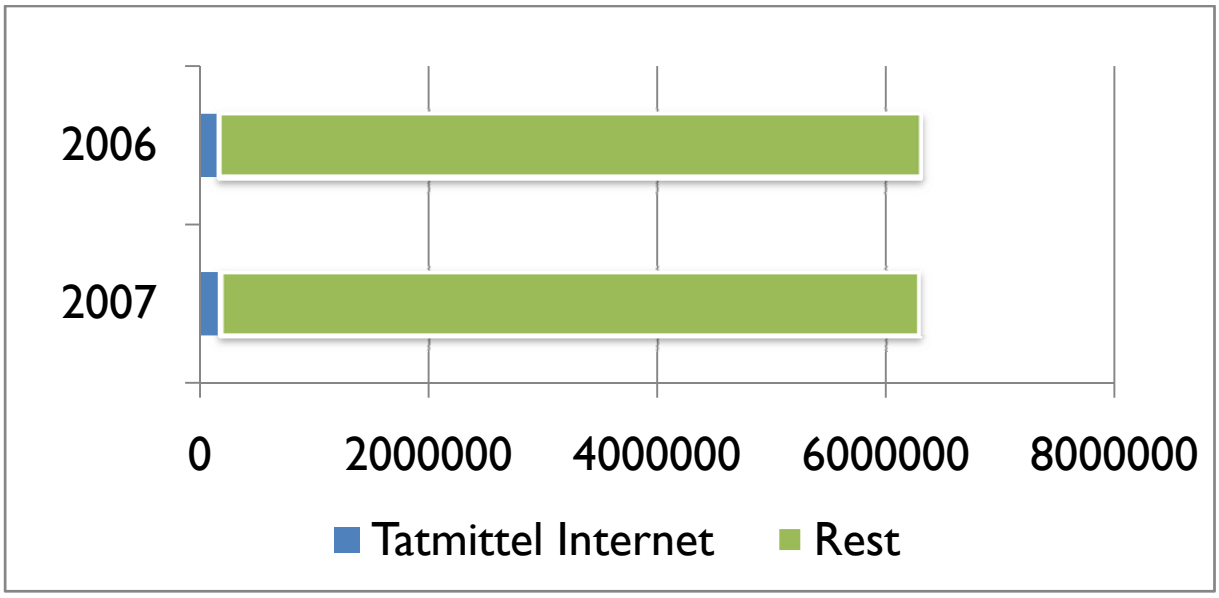
Sonstiger Warenkreditbetrug
Der umgedrehte Fall. Hier ist der Käufer der Böse. Er erwirbt Ware, mit dem Vorsatz sie nicht zu bezahlen.

Pornografische Erzeugnisse
Verbreitung von verbotener Pornografie: Gewalt, Tierpornographie, sexueller Missbrauch von Kindern.

Computerbetrug
Das sind zum Beispiel technische Manipulationen durch Dialer. Eine Software baut im Hintergrund teure Wählverbindung auf.

Leistungskreditbetrug / Leistungsbetrug
Analog Warenbetrug/Warenkreditbetrug, nur mit Dienstleistungen.

Anteil der Straftaten „Tatmittel Internet“



Insgesamt wurden 6.284.661 Straftaten verübt, letztes Jahr waren es 6.304.223. Dies entspricht einer Senkung um -0,3 %

2007: Mit Tatmittel Internet: 2,9 %, Rest 97,1 %

Methoden

Hier ist ein kurzer Überblick über die Methoden, mit welchen die Straftaten durchgeführt werden:

Bot-Netze

Unter einem Botnet oder Botnetz versteht man eine Gruppe von Software-Bots. Die Bots laufen auf vernetzten Rechnern, deren Netzwerkanbindung sowie lokale Ressourcen und Daten ihnen zur Verfügung stehen. Betreiber illegaler Botnetze installieren die Bots ohne Wissen der Inhaber auf Computern und nutzen sie für ihre Zwecke.

Aktuelles Beispiel: Festnahmen mit Folgen.

Im Februar wurden von den kanadischen Behörden 17 Personen festgenommen, die der Unterhaltung des größten Zombie-Netzwerks verdächtigt werden, das je im Land entdeckt wurde. Es wird angenommen, dass das Netzwerk über eine Million infizierte Computer in über 100 Ländern umfasste[16].

Im März wurde der 18-jährige Neuseeländer Owen Walker für die Nutzung von Computern für illegale Zwecke in 6 Anklagepunkten für schuldig befunden. Er gab zu, bei der Infizierung von 1,3 Millionen Computern weltweit eine tragende Rolle gespielt zu haben[17].

DoS-Angriffe, DDoS DRDoS, PDOS

Denial of Service, was so viel bedeutet wie „außer Betrieb setzen“. Ein Angriff mit dem Ziel, einen oder mehrere Dienste arbeitsunfähig zu machen. In der Regel geschieht dies durch die Überlastung des Dienstes. In diesem Zeitraum ist zum Beispiel eine Webseite nicht erreichbar. Viele große Sites wurden schon mit Angriffen bedacht.

Drive-By-Downloads

Ein Drive-by-Download bezeichnet das unbewusste Herunterladen von Software auf den Rechner eines Benutzers. Die geschieht meist über eine Schwachstelle des Browsers. Es reicht ein Aufruf der präparierten Webseite aus.

Exploits, Zero-Day-Angriffe

Ein Exploit (englisch to exploit - ausnutzen) ist ein Stück Software oder eine Sequenz von Befehlen, welches spezifische Schwächen beziehungsweise Fehlfunktionen eines anderen Computerprogramms ausnutzt.

Ein Exploit, das vor oder am selben Tag erscheint, an dem die Sicherheitslücke allgemein bekannt wird, nennt man Zero-Day-Exploit. Die Gefährlichkeit dieser Exploits rührt daher, dass zu diesem Zeitpunkt kaum ein Hersteller bzw. Entwickler in der Lage ist, die Sicherheitslücke zu schließen.

[16] Sophos: http://www.sophos.com/news/2008/02/botnet-busted.html
[17] Sophos: http://www.sophos.com/news/2008/04/owen-walker.html

Keylogger, SpyWare
Dient zur Aufzeichnung der Eingaben an der Tastatur des Opfers. Ziel ist z. B. das Aufzeichnen und Übermitteln von Passwörtern.

Phishing, Spear Phishing
Es handelt sich meist um kriminelle Handlungen, die Techniken des Social Engineering verwenden. Phisher geben sich als vertrauenswürdige Personen aus und versuchen durch gefälschte elektronische Nachrichten an sensible Daten, wie Benutzernamen und Passwörter für Online-Banking oder Kreditkarteninformationen, zu gelangen. Phishing-Nachrichten werden meist per E-Mail versendet. Unter Spear Phishing versteht man sehr gezielte Phishingangriffe. Bei dieser Form des Betrugs versenden die Phisher legitim wirkende E-Mails an sämtliche Angehörige oder Mitarbeiter eines bestimmten Unternehmens bzw. einer bestimmten Organisation oder Gruppe.

Pharming
Sie basiert auf einer Manipulation der DNS-Anfragen von, um den Benutzer auf gefälschte Webseiten umzuleiten. Es ist eine Weiterentwicklung des klassischen Phishings. Der Begriff "Pharming" rührt von dem Umstand her, dass die Pharming-Betrüger eigene große Server-Farmen unterhalten, auf denen gefälschte Webseiten abgelegt sind.

Spam
Wir hatten ja das Beispiel am Anfang mit 30.000 E-Mails. Wenn man es aber mit 1.000.000 E-Mails und einem verlockendem Angebot kombiniert. Zum Beispiel ein 250 Euro Produkt für nur 80 Euro. Natürlich per Vorkasse. Die meisten werden die E-Mail ignorieren. Viele ihr nicht vertrauen. Aber wenn nur jeder 1.000 darauf eingeht, haben Sie 1 Woche später ca. 80.000 Euro auf dem Konto. Sehr verlockend!

Sniffing
Beim Sniffing wird eine spezielle Software verwendet, um den Datenverkehr eines Netzwerkes zu empfangen. Mit der Auswertung dieser Daten können wichtige Informationen erspäht werden.

Typosquatting
Sie beruht darauf, dass eine Person eine Websiteadresse in einem Webbrowser versehentlich falsch eintippt und dann auf eine alternative Site geführt wird, die dem Typosquatter gehört. Oft enthalten diese Seiten dann ein Konkurrenzangebot, unpassende Werbung oder Schadcode. 0 / O oder l und I

WarDriving
Wardriving ist das systematische Suchen nach Wireless Local Area Networks mit Hilfe eines Fahrzeugs.

Virus
Ein Virus ist ein Programmcode, der mit dem Ziel geschrieben wurde, sich selbst zu replizieren. Er hängt sich selbst an ein „Hostprogramm“ an und versucht dann, sich von Computer zu Computer zu verbreiten.

Wurm

Der Wurm ist ein eigenständiges Programm, das sich selbstständig verbreiten kann. Würmer sind deshalb so gefährlich, weil sie sich unkontrollierbar vermehren. Sie nutzen zum Beispiel gern die Adressbücher der Opfer um sich selbst an alle E-Mailadressen zu versenden.

Trojaner

Trojanisches Pferd. Ein Computerprogramm, das einen offenen sichtbaren Nutzen hat, aber tatsächlich Schaden anrichtet.

Aktuelles Beispiel: Im März 2008 wurden bei der Supermarktkette Hannaford Bros Kreditkartennummern von 4,2 Millionen Kunden mithilfe von Schadcode, die auf den Servern von Filialen der Lebensmittelkette in Neuengland und Florida installiert war, gestohlen. Die Kreditkartendaten wurden anschließend ins Ausland versendet[18].

Fünf der weltweit aktivsten Computerhacker in Spanien gefasst.

Den jungen Männern im Alter von 16 bis 19 Jahren wird vorgeworfen seit 2006 mehr als 20.000 Websites sabotiert zu haben. Zu den Geschädigten zählten Telekomunternehmen, Regierungen und politische Parteien im In- und Ausland sowie die US-Weltraumbehörde NASA. Die Internetseiten wurden entweder lahm gelegt oder durch Protestbotschaften ersetzt. Die fünf Spanier kannten sich nicht persönlich, sprachen sich aber im Internet über ihre Aktionen ab. Ihnen drohen nun ein bis drei Jahre Haft[19].

Immer mehr Bedrohungen aus dem Internet

So entdeckt Sophos im Durchschnitt über 15.000 Webseiten pro Tag. Es sind nicht nur kleine Händler oder Webseiten betroffen. Im März wurde eine Fußballticket-Website für die EM 2008 von Hackern attackiert, um die Computer unvorsichtiger Fans zu infizieren[20].

[18] Hannaford: http://www.hannaford.com/Contents/News_Events/News/index.shtml
[19] Computerwoche, 19.05.2008: http://www.computerwoche.de/knowledge_center/security/1864161/
[20] Sophos: http://www.sophos.com/news/2008/03/euro2008.html

4. Schutzmaßnahmen

Das Gefahrenbewusstsein ist zurzeit noch nicht genügend entwickelt. Insbesondere bei den Privatpersonen suggeriert die Werbung einen schnellen problemlosen Zugang zum Internet. Doch gerade die „unerfahrenen" sind meist die Opfer von Phishing-Attacken oder E-Mails mit angehängtem Schadcode. Deswegen ist in erster Instanz die Sensibilisierung und Aufklärung das beste Mittel um den Gefahren aus dem Weg zu gehen oder erst gar nicht an sich ran zu lassen.

- Aufklärung / Beratung / Schulungen (Organisatorische Maßnahmen)
    - **Medienkompetenz**

      Es ist mehr als nur der sichere Umgang mit Medien. Verbunden ist damit auch die Fähigkeit der optimalen Ausnutzung. Digitale Medien sind im Vergleich zu analogen, wie Zeitung oder Bücher, wesentlich komplexer. Sie ermöglichen eine Interaktion zwischen Personen, Maschinen oder mit dem Medium selbst. Damit ist ein verantwortungsvoller, aber auch kritischer Umgang mit diesen Medien notwendig.
      In diesem Monat (Mai 2008) wurde eine 49-jährige Frau angeklagt, ein 13-jähriges Mädchen über MySpace beim Chatten[21] in den Suizid getrieben zu haben (2006). Die Angeklagte und Ihre Komplizin (Tochter) werden beschuldigt, das minderjährige MySpace-Mitglied gequält, schikaniert, verletzt und beschämt zu haben. Der Beschuldigten drohen bis zu 20 Jahre Haft.
      Insbesondere bei den Jugendlichen haben sich ein paar sehr bedenkliche „Spielarten" entwickelt. Ich möchte an dieser Stelle auf die morgigen Vorträge „Happy Slapping" Erscheinungsformen und Motive und „Was macht mein Kind im Internet" verweisen.
- Technisch
    - Hardware
        - Firewall

          Die Firewall überwacht den durch sie hindurch laufenden Datenverkehr und entscheidet anhand festgelegter Regeln, ob bestimmte Netzwerkpakete durchgelassen werden, oder nicht. Auf diese Weise versucht die Firewall das private Netzwerk bzw. das Netzsegment vor unerlaubten Zugriffen zu schützen.
    - Software
        - Aktuelles Betriebssystem

          Nur wenn Sie Ihren PC „up-to-date" halten, lassen sich Datenverluste, die Infektion mit neuen Viren und andere potenzielle Risiken vermeiden.
        - Anti-Viren-Software

[21] http://diepresse.com/home/techscience/internet/384186/index.do?_vl_backlink=/home/techscience/internet/index.do

        - „Persönliche Firewall“ (Desktop Firewall)
- Gesetze
    - Cybercrime-Konvention[22]

      Die am 08.11.2001 vom Ministerkomitee des Europarats verabschiedete Convention on Cybercrime wurde 15 Tage später, am 23.11.2001, von 30 Staaten, unter ihnen auch Deutschland und die nicht europäischen Staaten Kanada, Japan, Südafrika und die Vereinigten Staaten von Amerika, unterzeichnet. Die Cybercrime-Konvention soll einen Mindeststandard bei Gesetzen und Vorgehensweisen zur Bekämpfung “verschiedener Arten kriminellen Verhaltens gegen Computer Systeme, Netzwerke und Daten” schaffen. *Bis heute haben die Konvention 22 der 43 Unterzeichnerstaaten ratifiziert. Deutschland ist nicht darunter. Doch laut einem Beschluss der Bundesregierung[23] vom 28.09.2007 soll sich das ändern. Wenn Deutschland die Konvention ratifiziert, bedeutet das, dass bis zu 52 Staaten Zugriff auf die, mit dem Beginn der Vorratsdatenspeicherung am 01.08.2008 gesammelten Daten über deutsche Bürger erhalten. Zur Erinnerung: bei der Vorratsdatenspeicherung werden Daten über sämtliche Telefonverbindungen (Rufnummer, Zeit,…), Verbindungsaufbau mit dem Internet (Zeitpunkt, Internetadressen), E-Mail-Verkehr (IP und Mailadresse von Absender/Empfänger und Zugriffszeitpunkte auf das Postfach) sowie Fax- und SMS-Nachrichten (auch Lokalisierung) aller Bürger sechs Monate ohne Verdacht auf Vorrat gespeichert, was nicht von jedem Bürger als unproblematisch betrachtet wird.*

Nur eine physische Trennung der Daten vom Internet bietet Ihnen 100 % Schutz.

Persönliche Maßnahmen

- Das Betriebssystem immer auf den aktuellen Stand halten (automatische Updatefunktion)
- Anti-Viren Software installieren
- Firewall / persönliche Firewall (Desktop-Firewall) verwenden
- Sichere Passwörter verwenden und diese nicht in der Nähe des PCs aufbewahren. Ein Passwort sollte mindestens acht Zeichen haben und eine Kombination aus Buchstaben, Zahlen und Sonderzeichen sein.
- Keine E-Mailanhänge oder links von unbekannten Absendern öffnen
  Vorsicht! E-Mailadressen sind leicht zu fälschen. Auch Malware versendet gern SPAM automatisch an alle Kontaktadressen.
- Keine persönlichen Informationen oder Zugangsdaten preisgeben

[22] http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=185&CM=8&DF=1/14/2008&CL=GER
[23] http://www.bundesrat.de/cln_051/nn_8336/SharedDocs/Drucksachen/2007/0601-700/666-07,templateId=raw,property=publicationFile.pdf/666-07.pdf

- W-LAN: Verschlüsselung aktivieren, möglichst WPA/WPA2
- Achten Sie auf Ihre Hardware (Verlust) [24]

Bei den Unternehmen muss die Führung sensibilisiert werden. Sie müssen sich für ein vollständiges Sicherheitskonzept entscheiden, mit Leitlinien, die definierte Sicherheitsziele verfolgen und einer gesamtheitlichen Strategie[25]. Dies ist natürlich mit einem erhöhten Zeit- und Kostenaufwand verbunden, doch in fast allen Firmen – auch Einzelunternehmungen – ist das Funktionieren der IT-Systeme ein unabdingbarer Teil des Tagesgeschäfts.

Die IT-Sicherheit ist somit nicht als ein rein technischer Kostenfaktor zu sehen, sondern betriebswirtschaftlich existentiell.

Übrigens erlaubt das Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG) Schadenersatzansprüche gegenüber dem Vorstand, wenn dieser die Sorgfaltspflicht bei der Implementierung eines Risikomanagements verletzt hat.

Aber egal ob als Privatperson oder Unternehmen. Alle Maßnahmen müssen kontinuierlich erfolgen und bedürfen einer fortlaufenden Beobachtung und Pflege.

[24] polizei-beratung.de: http://www.polizei-beratung.de/file_service/documents/Hardware-Sicherheit.pdf
[25] BSI: http://www.bsi.de/gshb/webkurs/gskurs/seiten/s2500.htm

5. Anlaufstellen

„Praxistest“

Es wurden 30 Polizeidienststellen angerufen und denen ein Phishing-Fall geschildert.

Phishing ist eine Straftat: Ausspähen von Daten (§ 202a StGB, Vorbereiten des Ausspähens und Abfangens von Daten). Meist sind damit auch Verstöße gegen das Markengesetz verbunden.

63 % haben die Straftat nicht erkannt
29 % haben die Straftat als solche erkannt
8% wussten es nicht, aber auf Spezialisten verwiesen

37 % haben auf die Bank als Ansprechpartner verwiesen

Ob es Informationen im Internet über das Thema gibt, konnte nur jeder 5. eine zufrieden stellende Auskunft geben.

„Antworten“: (Gibt’s nicht, überfragt, Selbsthilfegruppen, Hilfsorganisationen, etc.)
„Hilfestellungen“: Kontoauszug abholen. Wenn nichts ist, einfach nächste Woche noch mal abrufen.

BSI - Bundesamt für Sicherheit in der Informationstechnik

Das Angebot wendet sich an die Nutzer und Hersteller von Informationstechnik. In erster Linie die öffentlichen Verwaltungen in Bund, Länder und Kommunen, aber auch Unternehmen und Privatanwender.

www.bsi.de

BSI für Bürger

Das Bundesamt für Sicherheit in der Informationstechnik bietet für Privatpersonen umfangreiche und gut aufbereitete Informationen.

www.bsi-fuer-buerger.de

BürgerCERT

Das Bürger-CERT informiert und warnt Bürger und kleine Unternehmen schnell und kompetent vor Viren, Würmern und Sicherheitslücken in Computeranwendungen. Aktuelle Warnmeldungen und Informationen werden per E-Mail versendet.

www.buerger-cert.de

jugendschutz.net

jugendschutz.net kontrolliert das Internet und hilft bei der Einhaltung des Jugendschutzes.

www.jugendschutz.net

Mit über 750 Beschwerden hat die Anzahl der Hotline-Hinweise im Januar einen neuen Rekordstand erreicht. Damit bearbeitet jugendschutz.net heute in einem Monat mehr Beschwerden als noch in 2000 innerhalb eines ganzen Jahres. Bei der Hälfte der eingehenden Meldungen handelte es sich in 2008 bisher um Pornoseiten, die verbotenerweise für Jugendliche zugänglich sind. Acht Prozent waren Hinweise auf die sexuelle Ausbeutung von Kindern im Netz. Deutlich zugenommen haben Anfragen zu Chats und sozialen Netzwerken wie SchülerVZ oder MySpace.[26]

[26] Jugendschutz.net: http://www.jugendschutz.net/materialien/sid08.html

Internet-Beschwerdestelle

Der Verband der deutschen Internetwirtschaft eco und die Freiwillige Selbstkontrolle Multimediadiensteanbieter FSM betreiben seit Jahren Hotlines zum Entgegennehmen von Beschwerden über illegale und schädigende Internetinhalte. Mit der gemeinsamen Webseite Internet-Beschwerdestelle.de bieten die Organisationen zum Ersten Mal Nutzern die Möglichkeit an, sich an einer Stelle über verschiedene Aspekte zur Förderung des sichereren Umgangs mit dem Internet zu informieren und Beschwerden entsprechend der Arbeitsteilung von eco und FSM einzureichen.

www.internet-beschwerdestelle.de

fsm

Die FSM ist ein Verein von Medienverbänden und Unternehmen der Online-Wirtschaft. Die Selbstkontrollorganisation bietet jedermann die Möglichkeit an, sich im Bereich des Jugendmedienschutzes über strafbare oder jugendgefährdende Inhalte im Netz zu beschweren oder Fragen zum Thema Jugendschutz im Internet zu stellen.

www.fsm.de

Kinder sicher im Netz

Eine gemeinsame Aktion der Polizeilichen Kriminalprävention der Länder und des Bundes (ProPK), der Freiwilligen Selbstkontrolle Multimedia (FSM) und der Deutschen Telekom AG zur Förderung der Internetkompetenz von Eltern.

www.polizei-beratung.de/vorbeugung/medienkompetenz/internet

klicksafe.de

Klicksafe ist eine Initiative des Safer Internet Programms der Europäischen Kommission. Es informiert Kinder, Jugendliche, Eltern, Multiplikatoren sowie Internetanbieter über Sicherheitsthemen und Entwicklungen im Internet.

www.klicksafe.de

Kommission für Jugendmedienschutz

Jugendgefährdende oder jugendbeeinträchtigende Internetinhalte können hier gemeldet werden.

www.kjm-online.de

polizei-beratung.de

Polizeiliche Kriminalprävention der Länder und des Bundes

www.polizei-beratung.de

Landesmedienanstalten

Bayern	Bayerische Landeszentrale für neue Medien http://www.blm.de/inter/de/pub/medienkompetenz.cfm
Bremen	Bremische Landesmedienanstalt http://www.bremische-landesmedienanstalt.de
Hessen	Hessische Landesanstalt für privaten Rundfunk http://www.lpr-hessen.de/default.asp?m=22
Baden-Württemberg	Landesanstalt für Kommunikation http://www.lfk.de/medienkompetenzausundfortbildung/main.html
Nordrhein-Westfalen	Landesanstalt für Medien http://www.lfm-nrw.de/medienkompetenz_neu/
Saarland	Landesmedienanstalt Saarland http://www.lmsaar.de/front_content.php?idcat=66
Sachsen-Anhalt	Landesrundfunkausschuss Sachsen-Anhalt http://www.lra.de/index.php?content=Medienkompetenzzentrum
Mecklenburg-Vorpommern	Landesrundfunkzentrale MV http://www.lrz-mv.de/medienkompetenz/
Rheinland-Pfalz	Landeszentrale für Medien und Kommunikation http://www.lmk-online.de/medienkompetenz/
Berlin	Medienanstalt Berlin http://www.mabb.de/start.cfm?content=Medienkompetenz
Brandenburg	Medienanstalt Brandenburg http://www.mabb.de/start.cfm?content=Medienkompetenz

6. Schlusswort

Immer mehr Lebensbereiche verändern sich durch das Internet, die Gesellschaft beginnt langsam das Internet als „normal“ zu betrachten und wird mehr und mehr miteinander vernetzt. Viele weitere Produkte und Dienstleistungen werden uns zukünftig zur Verfügung stehen, dabei wird das uns jetzt bekannte Internet sich wandeln, es wird zu einem Teil von uns. So selbstverständlich, wie jeder von uns ein Handy in der Tasche hat, werden wir zukünftig aufs Internet zugreifen. Genauso selbstverständlich wird sich die Internet-Kriminalität entwickeln.

Heute

17:00 - 18:00 „Präventiver Jugendmedienschutz – Sicheres Chatten am Beispiel des moderierten Kinderchats von Seitenstark“
http://www.praeventionstag.de/Dokumentation.cms/437

Morgen

09:00 - 10:00 "Kompetente Onlineberatung durch Ehrenamtliche - ein Praxisbericht"
http://www.praeventionstag.de/Dokumentation.cms/436

11:00 - 12:00 "Happy Slapping" - Erscheinungsformen und Motive. Empirische Ergebnisse und Anregungen für die Prävention.
http://www.praeventionstag.de/Dokumentation.cms/439

14:00 - 15:00 Was macht mein Kind im Internet? Worin liegt die Gefährdung? Medienerziehungstipps, Medienempfehlungen und Hilfsangebote
http://www.praeventionstag.de/Dokumentation.cms/440

Raum für Notizen: