Einführung in die Informatik, Algorithmen und Datenstrukturen

Thema 9

Informatik, Mensch, Gesellschaft

Meldung 14.01.09

Computerstörung bei der Bahn
Eine Störung im Computersystem der Bahn hat den Ticketverkauf praktisch lahmgelegt und in weiten Teilen Deutschlands für Verspätungen gesorgt. Ursache der Behinderungen war ein Netzwerkausfall, wie der bundeseigene Konzern in Berlin mitteilte. Tausende Kunden konnten an den meisten Automaten, an Schaltern und im Internet keine Fahrkarten mehr kaufen. Betroffen waren stundenlang auch Reiseauskunfts- und Anzeigesysteme auf den Bahnhöfen, wodurch es bundesweit zu Verzögerungen im Zugverkehr kam.

Informatik und Gesellschaft

Datenschutz

Urheberrecht

Jugendschutz

Teledienstgesetz

E-Commerce

Softwarelizenzen

online-Banking

Identity-Management

E-Goverment

Viren- Würmer -Trojaner

Phishing

Fernmeldegeheimnis

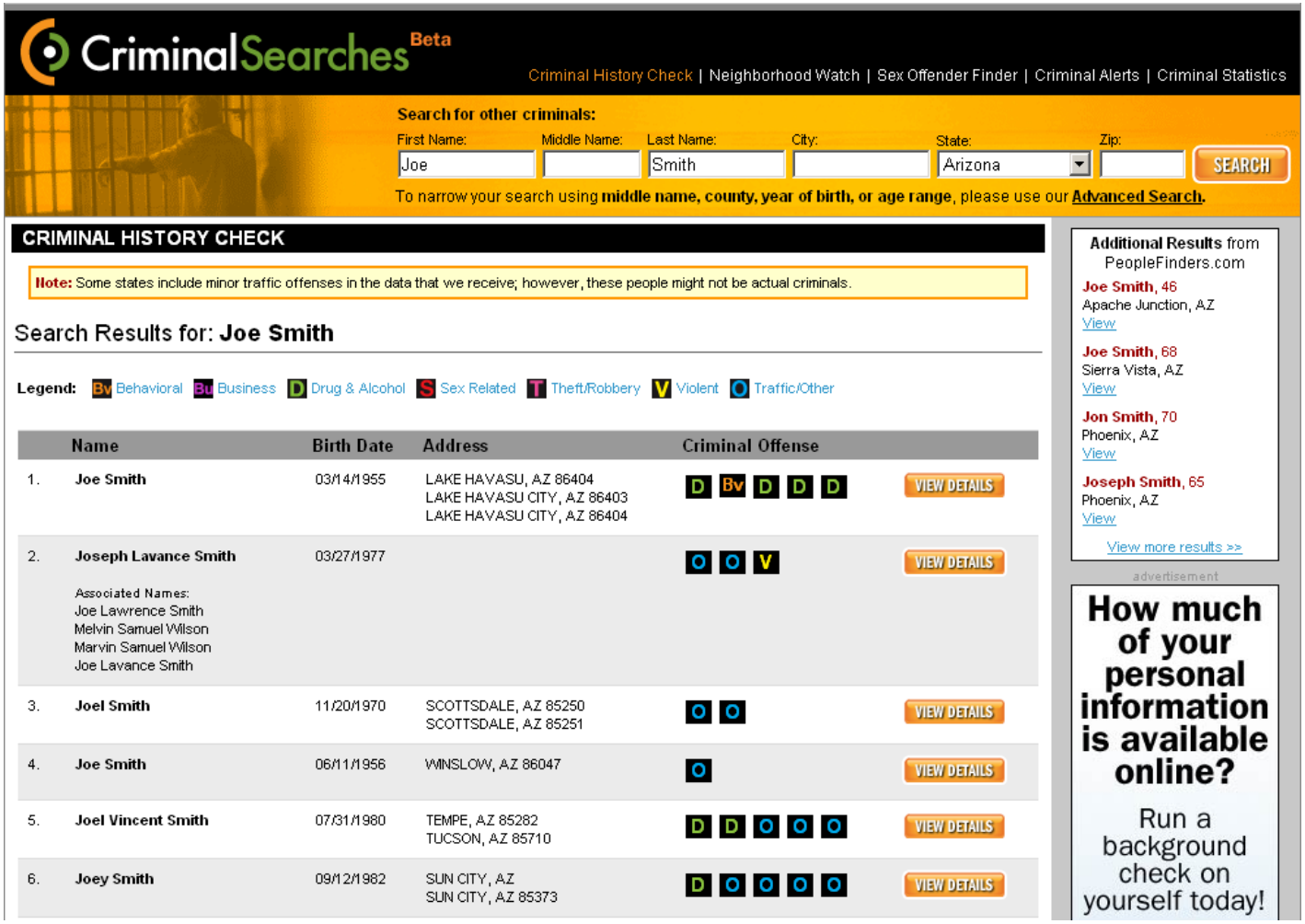
Bereits die Weimarer Reichsverfassung von 1919 garantierte den Bürgern im Artikel 117 das Fernsprechgeheimnis.
Das Fernmeldegeheimnis im Grundgesetz von 1949 gehört zu den Grundrechten (Art. 10 GG), allerdings besteht die Möglichkeit, das Fernmeldegeheimnis durch ein einfaches Gesetz einzuschränken, d. h. der Staat darf sich in bestimmten gesetzlich geregelten Situationen Kenntnis von Inhalt oder Umständen der Kommunikation verschaffen.

Fernmeldegeheimnis

Durch Gesetz vom 24. Juni 1968, als Teil der Notstandsgesetze von 1968, erhielt der Artikel diese Fassung:

(1) Das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis sind unverletzlich.
(2) Beschränkungen dürfen nur auf Grund eines Gesetzes angeordnet werden. Dient die Beschränkung dem Schutze der freiheitlichen demokratischen Grundordnung oder des Bestandes oder der Sicherung des Bundes oder eines Landes, so kann das Gesetz bestimmen, daß sie dem Betroffenen nicht mitgeteilt wird und daß an die Stelle des Rechtsweges die Nachprüfung durch von der Volksvertretung bestellte Organe und Hilfsorgane tritt.

Daten - international



CriminalSearches Beta

Criminal History Check | Neighborhood Watch | Sex Offender Finder | Criminal Alerts | Criminal Statistics

Search for other criminals:

First Name: Joe | Middle Name: | Last Name: Smith | City: | State: Arizona | Zip: | SEARCH

To narrow your search using **middle name, county, year of birth, or age range**, please use our **Advanced Search**.

CRIMINAL HISTORY CHECK

Note: Some states include minor traffic offenses in the data that we receive; however, these people might not be actual criminals.

Search Results for: **Joe Smith**

Legend: Bv Behavioral | Bu Business | D Drug & Alcohol | S Sex Related | T Theft/Robbery | V Violent | O Traffic/Other

	Name	Birth Date	Address	Criminal Offense	
1.	**Joe Smith**	03/14/1955	LAKE HAVASU, AZ 86404 LAKE HAVASU CITY, AZ 86403 LAKE HAVASU CITY, AZ 86404	D Bv D D D	VIEW DETAILS
2.	**Joseph Lavance Smith** Associated Names: Joe Lawrence Smith Melvin Samuel Wilson Marvin Samuel Wilson Joe Lavance Smith	03/27/1977		O O V	VIEW DETAILS
3.	**Joel Smith**	11/20/1970	SCOTTSDALE, AZ 85250 SCOTTSDALE, AZ 85251	O O	VIEW DETAILS
4.	**Joe Smith**	06/11/1956	WINSLOW, AZ 86047	O	VIEW DETAILS
5.	**Joel Vincent Smith**	07/31/1980	TEMPE, AZ 85282 TUCSON, AZ 85710	D D O O O	VIEW DETAILS
6.	**Joey Smith**	09/12/1982	SUN CITY, AZ SUN CITY, AZ 85373	D O O O O	VIEW DETAILS

Additional Results from PeopleFinders.com

Joe Smith, 46
Apache Junction, AZ
View

Joe Smith, 68
Sierra Vista, AZ
View

Jon Smith, 70
Phoenix, AZ
View

Joseph Smith, 65
Phoenix, AZ
View

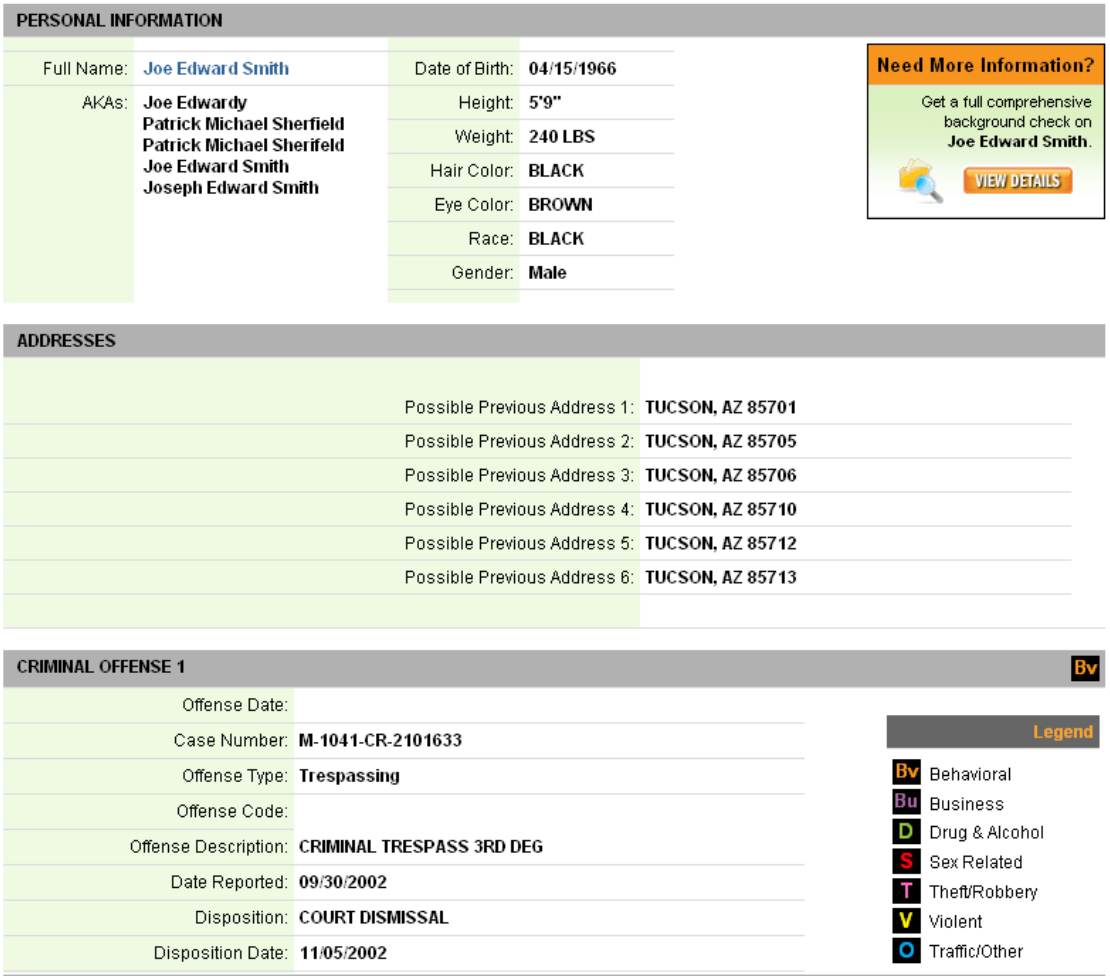
View more results >>

advertisement

How much of your personal information is available online?

Run a background check on yourself today!

Daten - international



PERSONAL INFORMATION

Full Name:	Joe Edward Smith	Date of Birth:	04/15/1966
AKAs:	Joe Edwardy Patrick Michael Sherfield Patrick Michael Sherifeld Joe Edward Smith Joseph Edward Smith	Height:	5'9"
		Weight:	240 LBS
		Hair Color:	BLACK
		Eye Color:	BROWN
		Race:	BLACK
		Gender:	Male

ADDRESSES

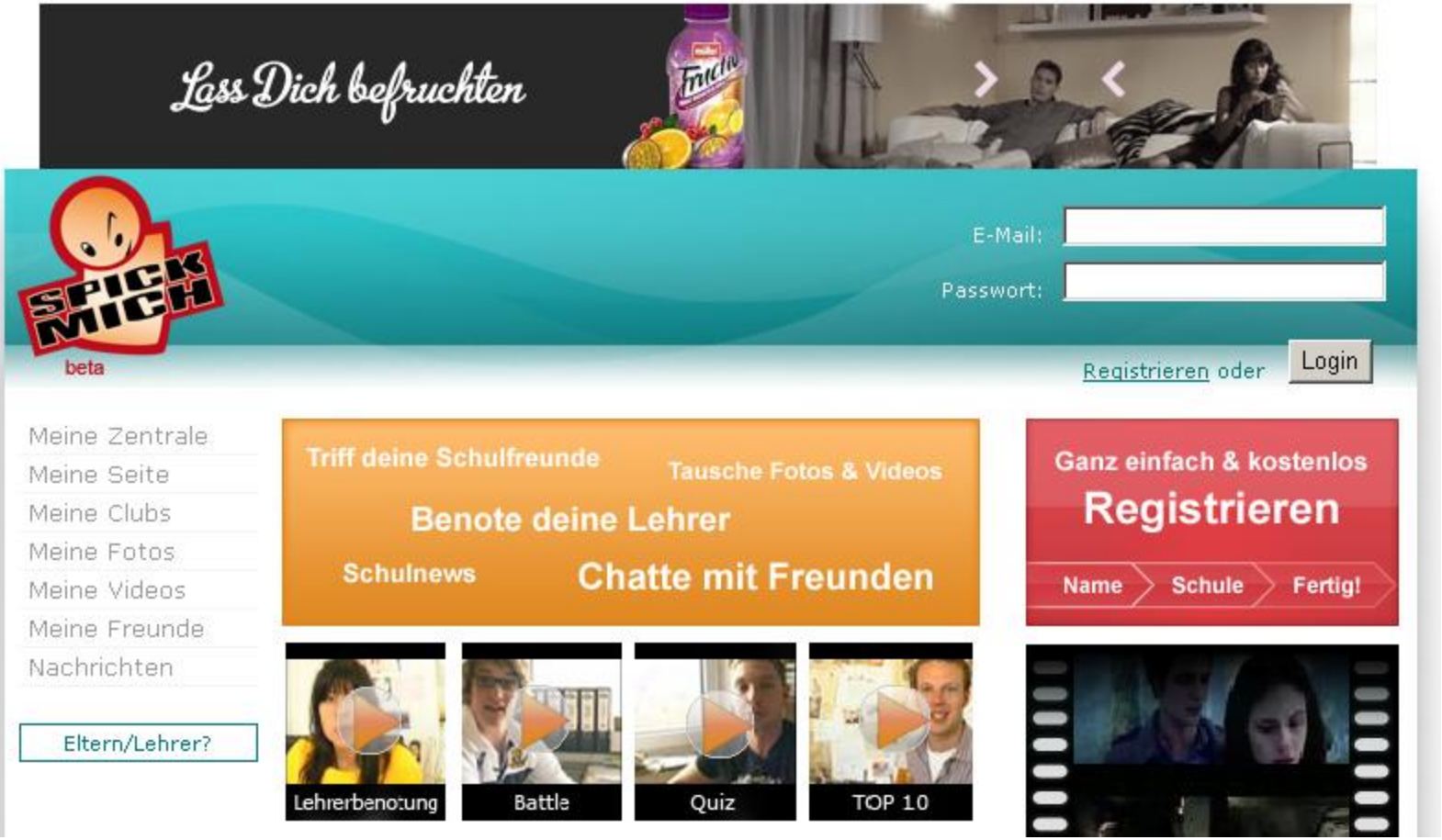
Possible Previous Address 1:	TUCSON, AZ 85701
Possible Previous Address 2:	TUCSON, AZ 85705
Possible Previous Address 3:	TUCSON, AZ 85706
Possible Previous Address 4:	TUCSON, AZ 85710
Possible Previous Address 5:	TUCSON, AZ 85712
Possible Previous Address 6:	TUCSON, AZ 85713

CRIMINAL OFFENSE 1 Bv

Offense Date:	
Case Number:	M-1041-CR-2101633
Offense Type:	Trespassing
Offense Code:	
Offense Description:	CRIMINAL TRESPASS 3RD DEG
Date Reported:	09/30/2002
Disposition:	COURT DISMISSAL
Disposition Date:	11/05/2002

Legend

- Bv Behavioral
- Bu Business
- D Drug & Alcohol
- S Sex Related
- T Theft/Robbery
- V Violent
- O Traffic/Other


Lass Dich befruchten
SPICK MICH
beta
E-Mail:
Passwort:
Registrieren oder
Login
Meine Zentrale
Meine Seite
Meine Clubs
Meine Fotos
Meine Videos
Meine Freunde
Nachrichten
Eltern/Lehrer?
Triff deine Schulfreunde
Tausche Fotos & Videos
Benote deine Lehrer
Schulnews
Chatte mit Freunden
Ganz einfach & kostenlos
Registrieren
Name
Schule
Fertig!
Lehrerbenotung
Battle
Quiz
TOP 10

Problemstellung

„Der Einsatz von Informatiksystemen wirft neuartige rechtliche Fragestellungen auf, die vor allem darauf beruhen, dass das Erfassen, Speichern und Auswerten von Informationen in einer bisher nicht gekannten Fülle und Schnelligkeit betrieben werden kann und im Internet keine Landesgrenzen mehr gelten.“

/Bernhard Koerber in: LOG IN 19 (1999) Heft 5, S. 3/

Ist das Internet ein rechtsfreier Raum?

Begriffsdefinitionen

Datenschutz:

ist die Verhinderung des Datenmissbrauchs beim Umgang mit **personenbezogenen Daten.**

Datensicherheit:

umfasst alle organisatorischen und technischen Maßnahmen zum Schutz von Daten vor Verlust und Verfälschung sowie vor unberechtigtem Zugriff.

Bundesdatenschutzgesetz - Begriffe

§ 1 Zweck und Anwendungsbereich des Gesetzes

Zweck dieses Gesetzes ist es, **den einzelnen davor zu schützen, dass er durch den Umgang mit seinen personenbezogenen Daten in seinem Persönlichkeitsrecht beeinträchtigt wird**.

§ 3 Weitere Begriffsbestimmungen

(1) **Personenbezogene Daten** sind Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener).

Bundesdatenschutzgesetz - Begriffe

(2) Eine **Datei** ist

1. eine Sammlung personenbezogener Daten, die durch automatisierte Verfahren nach bestimmten Merkmalen ausgewertet werden kann (automatisierte Datei),oder

2. jede sonstige Sammlung personenbezogener Daten, die gleichartig aufgebaut ist und nach bestimmten Merkmalen geordnet, umgeordnet und ausgewertet werden kann (nicht-automatisierte Datei).

(3) Eine **Akte** ist jede sonstige amtlichen oder dienstlichen Zwecken dienende Unterlage; dazu zählen auch Bild- und Tonträger. Nicht hierunter fallen Vorentwürfe und Notizen, die nicht Bestandteil eines Vorgangs werden sollen.

Bundesdatenschutzgesetz - Begriffe

(4) **Erheben** ist das Beschaffen von Daten über den Betroffenen.
(5) **Verarbeiten** ist das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Im einzelnen ist, ungeachtet der dabei angewendeten Verfahren
(6) **Nutzen** ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt.
(7) **Anonymisieren** ist das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.
(8) **Speichernde Stelle** ist jede Person oder Stelle, die personenbezogene Daten für sich selbst speichert oder durch andere im Auftrag speichern lässt.

Bürger-Daten

Montag, 23. Juni 2008 /Quelle: http://www.n-tv.de/983923.html/

Bürger-Daten offen im Netz

Bürger-Daten aus einer Reihe kommunaler Meldeämter sollen einem TV-Bericht zufolge im Internet jahrelang frei zugänglich gewesen sein. Die verantwortliche Softwarefirma habe die Zugangscodes auf ihrer eigenen Homepage veröffentlicht, berichtete das ARD-Fernsehmagazin "Report München".

Ein Test bei fünf Gemeinden ergab demnach, dass binnen Sekunden per Computer Daten ahnungsloser Bürger geliefert wurden - von Familienstand über Geburtsdatum bis zur Religionszugehörigkeit. Laut "Frankfurter Rundschau" griffen aufgrund des Fehlers Unbefugte auf Einwohnerdaten in Potsdam, Neuhardenberg und Henningsdorf zu.

Wer mit den öffentlich zugänglichen Passwörtern in die Computer vordrang, konnte "Report München" zufolge dort auch Passfotos der abgefragten Personen downloaden.

Studenten-Daten

Persönliche Daten von etwa 44.000 Studenten der Otto-von-Guericke-Universität Magdeburg waren zehn Tage lang im Internet öffentlich zugänglich.

Nach Angaben des Universitätskanzlers Wolfgang Lehnecke ist der Vorfall auf den Fehler eines Mitarbeiters zurückzuführen. Die Daten waren seit dem 9. Mai auf einem öffentlich zugänglichen Server zu finden. Nachdem aus den Reihen der Studenten ein Hinweis einging, wurden die Daten am 19. Mai gelöscht. Lehnecke sprach von einem "bitteren Vorfall". Eine Arbeitsgruppe, in die auch der Studentenrat einbezogen ist, soll weitere Konsequenzen vermeiden. Es sollen neue Verschlüsselungen eingeführt werden, um die Datensicherheit zu gewährleisten. Bis dahin soll es keine Aushänge der Noten mehr geben. Die müssten sich die Studenten vorerst beim Prüfungsamt abholen.

/Quelle: www.mdr.de/

Online-Durchsuchungen

- ONLINE-DURCHSUCHUNG: Die Überwachung privater Computer wird möglich. Das Bundesverfassungsgericht hat dafür in einem Grundsatzurteil enge Grenzen vorgegeben. Nur bei einer konkreten Gefahr und bei schwersten Straftaten dürfen die Ermittler mit Genehmigung eines Richters heimlich in einen Computer eindringen.
Eine Manipulation der Rechner vor Ort soll den Fahndern aber nicht erlaubt werden. Die technischen Voraussetzungen für die Überwachung dürfen nur über Datenleitung geschaffen werden, etwa über die heimliche Online-Installation einer entsprechenden Software.

/Quelle: www.n-tv.de/

Vorratsdatenspeicherung

Vorratsdatenspeicherung

Gespeichert werden zahlreiche Verkehrsdaten, die Aufschluss über die Kommunikation von Bürgern geben. Dazu zählen
- Telefonnummern von Anrufer und Angerufenem
- Uhrzeit und Dauer der Gespräche
- bei Mobilfunkgesprächen die Orte von Anrufer und Angerufenem
- E-Mail- und IP-Adressen von Sendern und Empfängern
- Verbindungsdaten bei der Internetnutzung.

Betroffen von der Speicherung sind auch SMS- oder Multimedia-Nachrichten. Gespeichert werden grundsätzlich Verbindungsdaten und keine Inhalte der Kommunikation. So soll beim Internet nur der Zugang erfasst werden, nicht der Aufruf einzelner Seiten.

/Quelle: www.n-tv.de, 30.11.2007/

Überwachung

Dein Handy weiß, wohin Du gehst!

Elektronische Überwachung von Personen (Kinder)

Systeme:

Track your Kid: Ortung des Handys

Sentinel Watch: Armbanduhr, die eine SMS versendet, wenn das Kind den vorgegebenen Schulweg verlässt oder versucht die Armbanduhr abzunehmen (GSM – Ortung)

Phonetracker: Eltern definieren Bereiche, in denen sich das Kind aufhalten darf. Das Handy des Kindes kann angerufen werden mit Klingeltonunterdrückung – Belauschen des Kindes. (Handy-Zusatzgerät)

E-Goverment – die digitale Verwaltungsära

Elektronische Verwaltung

z.B.

- Melderegister,
- Kraftfahrzeugregister,
- Finanzbehörden,
- Grundbuchregister,
- Gebührenverwaltung,
- …

E-Goverment – Zugriffsrechtemanagement

Für jeden im Netz tätigen Mitarbeiter wird ein zentrales, stets eindeutiges **Benutzer- und Rechteprofil** erstellt.

Mögliche Berechtigungsträger: Chipkarten

alternativ: biometrische Merkmale (Zuverlässigkeit?)

➔ neue Dimension der Informationsvorhaltung und Kontrolle

Rechtlicher Rahmen der Internetnutzung

- **Strafrecht**
  Für alle Taten, die im Internet in Deutschland begangen werden, kommt das deutsche Strafrecht zur Anwendung.
- **Urheberrecht**
  Alle Werke der Literatur, Wissenschaft und Kunst, wenn sie durch persönliche, geistige Schöpfung entstanden sind, sind auch im Internet durch das Urheberrechtsgesetz geschützt.
- **Jugendschutz**
  Die Verbreitung von Inhalten, die die physische und/oder geistige Entwicklung von Minderjährigen beeinträchtigen können muss durch geeignete Maßnahmen unterbunden werden.

Alles, was außerhalb des Internets strafbar ist, ist auch innerhalb des Internets strafbar.

Internetnutzung und Schule

- Für die Schüler sollten altersdifferenzierte Zugangsberechtigungen geschaffen werden.
- Die Eltern sollten in die Erziehung zum verantwortlichen Internetzugang mit einbezogen werden.
- Beim Web-Publishing verhindert die Einhaltung des Persönlichkeits- und Datenschutzes die mögliche Identifizierung der Schüler durch Informationen auf der Website.

Quelle: Leitfaden – Internetverantwortung an Schulen
Bertelsmann Stiftung 2000
http://www.internet-verantwortung.de/dad.html

Internetnutzung und Schule

RdErl. MK vom 11.10.1991, geändert 25.11.1991 (Schnellbrief Nr.2)(Auszüge)

>>>Lehrer und Erzieher haben in Ausübung ihrer beruflichen Tätigkeit eine umfassende Fürsorge- und Aufsichtspflicht. Sie treffen Vorsorge, dass die ihnen anvertrauten Kinder und Jugendlichen **weder geistigen, sittlichen noch körperlich -materiellen Schaden erleiden**.

>>>Die ***Aufsichtspflicht der Schule*** erstreckt sich auf die Zeit, in der die Schüler am **Unterricht oder an sonstigen Schulveranstaltungen teilnehmen**. Dazu gehören eine angemessene Zeit vor Beginn und nach Beendigung des Unterrichts oder sonstiger Schulveranstaltungen sowie die Pausen und Freistunden.

Internetnutzung durch Kinder

/www.internauten.de/

Internetnutzung für Lehrer

/www.klicksave.de/

Computerkriminalität

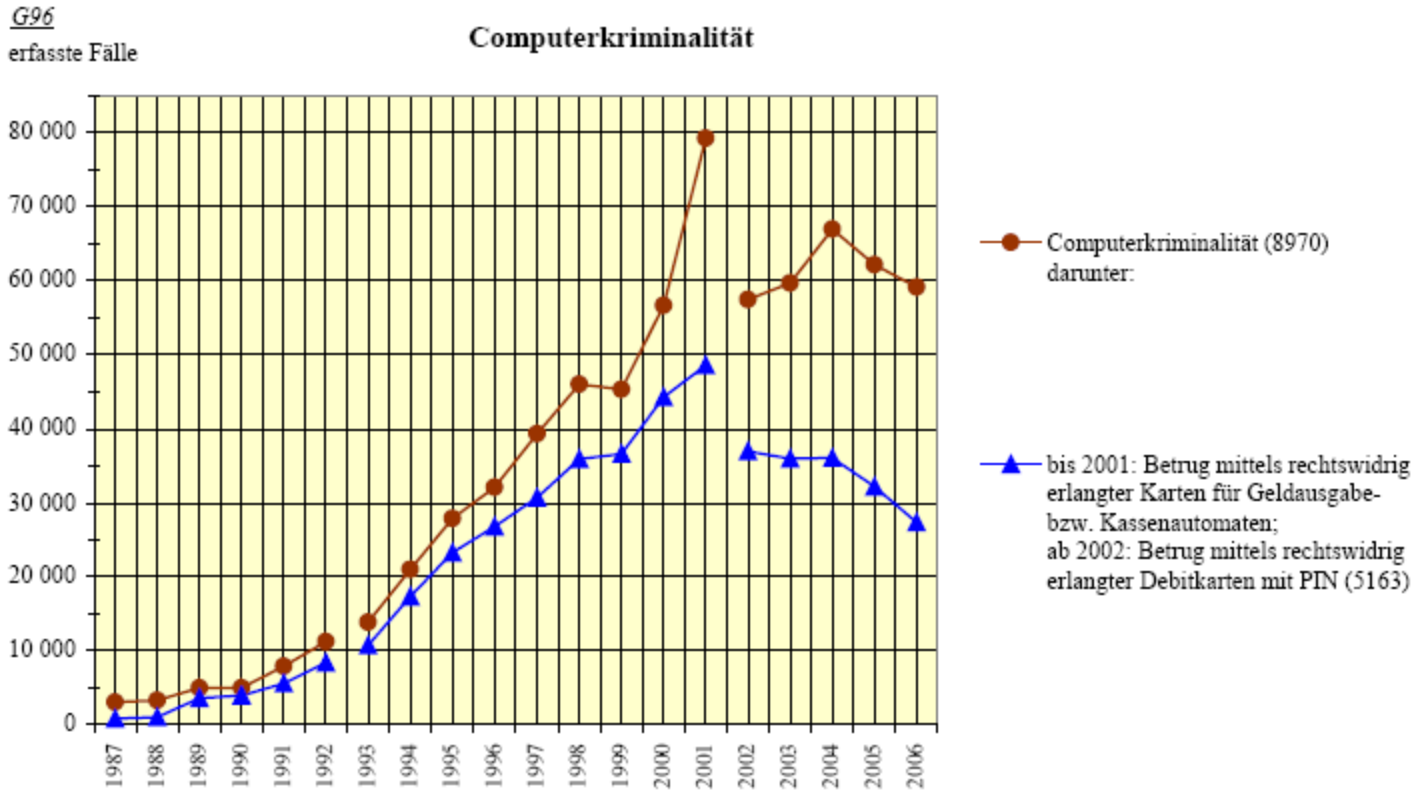
"Cybercrime hat sich zu einer eigenständigen Kriminalitätskategorie mit einer potenziellen Bedrohung für die öffentliche Sicherheit in der elektronischen Informationsgesellschaft entwickelt."

Innenminister Otto Schily, 11.06.2002

Computerkriminalität

- **Ausspähen von Daten**
  (z.B. Verrat von Geschäftsinterna)
- **Datenveränderung bzw. Computersabotage**
  (Sachbeschädigung)
- **Softwarepiraterie**
  (unautorisierte Speicherung, Vervielfältigung oder Verbreitung von Software)
- **Computerbetrug**
  (Abrechnungsmanipulation, Bilanzmanipulation, Kontostandsmanipulation)

Computerkriminalität



Hinweis:
1987 – 1990: alte Länder
1991 – 1992: alte Länder mit Berlin
ab 1993: Bundesgebiet insgesamt
1998: Wegen zusätzlicher Aufnahme von Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten (Schlüssel: 5179) ist ein Vergleich der Computerkriminalität (8970) zum Vorjahr beeinträchtigt.

/Quelle: Polizeiliche Kriminalstatistik 2006/

Computerkriminalität

T232

Schlüs-sel	Straftaten(gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2006	2005	absolut	in %	2006	2005
8970	Computerkriminalität	59 149	62 186	-3 037	-4,9	47,1	48,1
	davon:						
5163	Betrug mittels rechtswidrig erlangter Debitkarten mit PIN	27 347	32 232	-4 885	-15,2	40,6	40,9
5175	Computerbetrug -§263a StGB-	16 211	15 875	336	2,1	48,9	48,7
5179	Betrug mit Zugangsberechtigungen zu Kommunikationsdiensten	5 822	5 788	34	0,6	57,7	64,4
5430	Fälschung beweiserheblicher Daten, Täuschung im Rechtsverkehr bei Datenverarbeitung -§§ 269, 270 StGB-	2 460	1 012	1 448	143,1	44,9	46,7
6742	Datenveränderung, Computersabotage -§§ 303a, 303b StGB-	1 672	1 609	63	3,9	29,0	35,9
6780	Ausspähen von Daten	2 990	2 366	624	26,4	43,8	42,2
7151	Softwarepiraterie (private Anwendung z.B. Computerspiele)	1 920	2 667	-747	-28,0	96,7	98,7
7152	Softwarepiraterie in Form gewerbsmäßigen Handelns	727	637	90	14,1	98,3	96,9

/Quelle: Polizeiliche Kriminalstatistik 2006/

Computerkriminalität

Fallentwicklung und Aufklärung (Tabelle 05)

Bereich: Bundesgebiet insgesamt **ohne** Bayern und Niedersachsen

T240

Schlüs-sel	Straftaten(gruppen)	erfasste Fälle		Veränderung		Aufklärungsquote	
		2006	2005	absolut	in %	2006	2005
----	Straftaten insgesamt	150 785	118 036	32 749	27,7	84,0	84,9
1430	Verbreitung pornographischer Schriften (Erzeugnisse)	5 351	5 624	-273	-4,9	78,5	76,0
5100	Betrug	124 501	93 816	30 685	32,7	86,0	86,1
5112	sonstiger Warenkreditbetrug	15 555	10 322	5 233	50,7	94,8	94,3
5113	Warenbetrug	78 235	53 092	25 143	47,4	95,3	94,2
5171	Leistungsbetrug	3 153	800	2 353	294,1	88,3	84,4
5172	Leistungskreditbetrug	5 235	2 337	2 898	124,0	47,9	77,6
5175	Computerbetrug	8 285	8 168	117	1,4	41,8	35,6
5189	sonstige weitere Betrugsarten	8 694	13 207	-4 513	-34,2	69,9	88,2
7150	Straftaten gegen Urheberrechtsbestimmungen	10 286	10 432	-146	-1,4	85,5	92,6

Bei Straftaten mit Tatmittel Internet wurden teils kräftige Anstiege registriert. Dies könnte unter anderem auch auf eine verbesserte Erfassung der Sonderkennung "Tatmittel Internet" zurückzuführen sein.

/Quelle: Polizeiliche Kriminalstatistik 2006/

Datensicherheit

Vertraulichkeit: Die Vertraulichkeit der Daten ist gefährdet, wenn Unbefugte Zugriff zu schutzwürdigen Informationen enthalten. Nur der befugte Besitzer/Empfänger darf auf die Daten zugreifen.

Datenintegrität: Die Integrität der Daten ist gefährdet, wenn Informationen verfälscht oder unvollständig dargestellt und gespeichert werden können. Daten müssen gegen jede Art von unberechtigter Modifikation geschützt werden.

Verfügbarkeit: Die Verfügbarkeit der Daten ist gefährdet, wenn Informationen missbräuchlich oder irrtümlich gelöscht werden können. In Netzwerken kann der ständige unberechtigte Aufruf eines Dienstes zur Sperrung für berechtigte Anfragen führen.

Datensicherheit

Verbindlichkeit: Die Verbindlichkeit sichert, dass ein Empfänger eine Nachricht auch erhalten hat.

Anonymität: Es muss möglich sein, zu verbergen, wer mit wem wie oft kommuniziert oder wie oft jemand auf eine Datei zugegriffen hat. Dieses Kriterium steht im Widerspruch zur Authentizität.

Gesetzliche Aufbewahrungspflichten von Daten

Die Paragraphen 257 des Handelsgesetzbuches und 147 Abgabenverordnung verpflichten Unternehmer, Unterlagen bis zu einer bestimmten Frist aufzubewahren. Nach dem Steuerrecht gibt es dabei zwei Aufbewahrungsfristen:

6 Jahre z.B. für:

- empfangene Handels- und Geschäftsbriefe,
- Lieferscheine, Finanzberichte, Steuererklärungen, Bilanzunterlagen

10 Jahre z.B. für:

- Lohnbelege, Kassenbücher
- Reisekostenabrechnungen, Gewinn- und Verlustrechnungen,

Diese Fristen gelten auch für elektronisch gespeicherte Unterlagen!

Gesetzliche Aufbewahrungspflichten von Daten

Problem

Nicht nur die Daten müssen aufbewahrt werden, sondern es muss auch Hardware und Software zur Verfügung stehen, um diese Daten zu verarbeiten

Datensicherheit – auch bei der Entsorgung

Ein wesentlicher Aspekt bei der Datensicherheit besteht auch in der Entsorgung von Computern und Datenträgern.

Untersuchungen haben gezeigt, dass gebrauchte Festplatten häufig noch (teilweise sensible) Daten enthalten.

Datensicherheit – Regeln für die Erhöhung der Passwortsicherheit

1. ein Passwort sollte mind. 6 (besser 8) Zeichen enthalten
2. das Passwort sollte aus Buchstaben, Ziffern und Sonderzeichen bestehen (auch Leerzeichen)
3. Sonderzeichen sollten sich nicht am Ende des Passwortes befinden
4. Wörter und Daten aus dem persönlichen Umfeld vermeiden
5. Wörter, die im Duden oder Lexika stehen sollten nicht verwendet werden
6. Passwort verfremden (z.B. o durch 0 ersetzen)
7. für jeden Zugang sollte ein gesondertes Passwort verwendet werden
8. Passworte sollten nicht gespeichert werden

Gefahren bei der Online-Kommunikation

- Der Angreifer versucht sich auf verschiedenen Wegen interne Passwörter anzueignen, um sie für weitere Angriffe zu nutzen.
- Der Angreifer versucht, Daten auf dem Weg von A nach B zu manipulieren.
- Der Angreifer versucht Kontrolle über einen fremden Rechner zu erhalten.
- Verlust der Daten durch Viren.

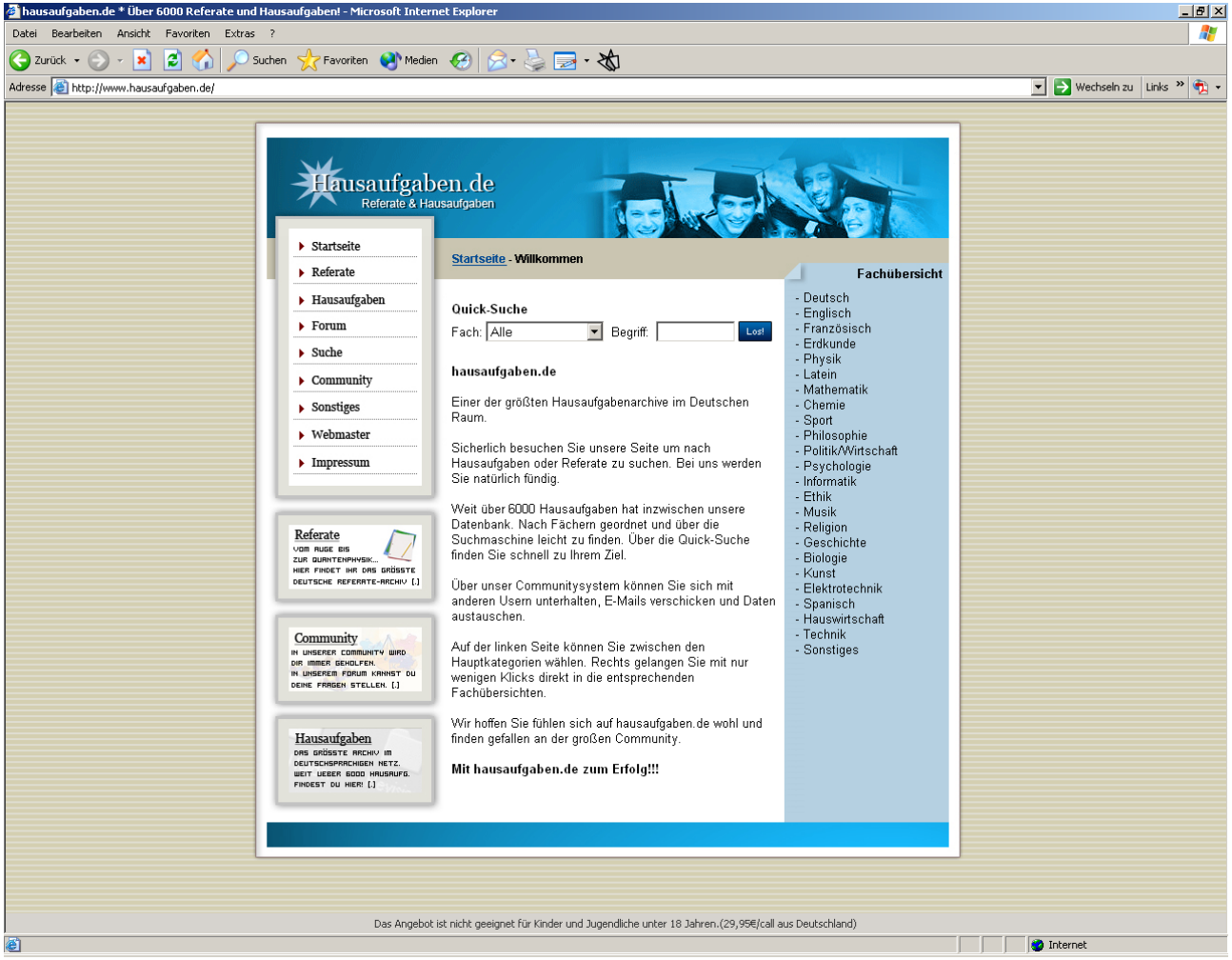
Quelle: www.sicherheit -im-internet.de

Internetsicherheit

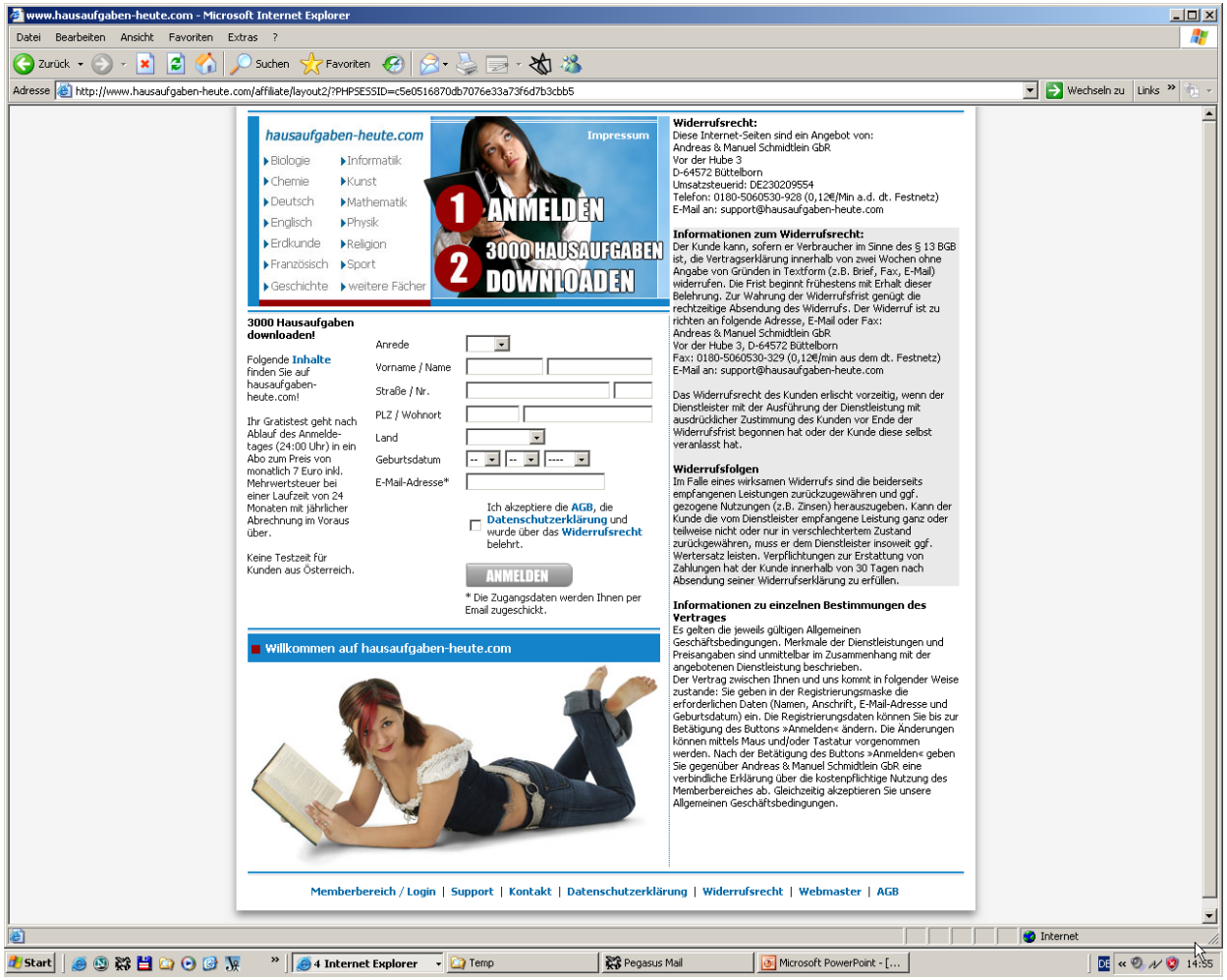
Was verraten wir im Netz?

- E-Mail-Adresse: nennt Provider oder Arbeitgeber
- eigene Website: liefert oft Lebensdetails und über die Domain-Registrierung die postalische Adresse
- Beiträge in Newsgroups und Chatrooms: erlauben Rückschlüsse auf Interessen, Kenntnisse und ggf. technische Probleme von Administratoren
- viele Server halten Aktivitäten und Verbindungsdaten aller Besucher in Logfiles fest
- E-Kommerce-Sites: Kreditkartennummern, Bankverbindungen, Profile über das Surf und Kaufverhalten

Kostenpflichtige Internetangebote



Kostenpflichtige Internetangebote



Kostenpflichtige Internetangebote

Domaindaten

Domain:	hausaufgaben.de
Letzte Aktualisierung:	06.01.2005

Domaininhaber

Der Domaininhaber ist der Vertragspartner der DENIC und damit der an der Domain materiell Berechtigte.

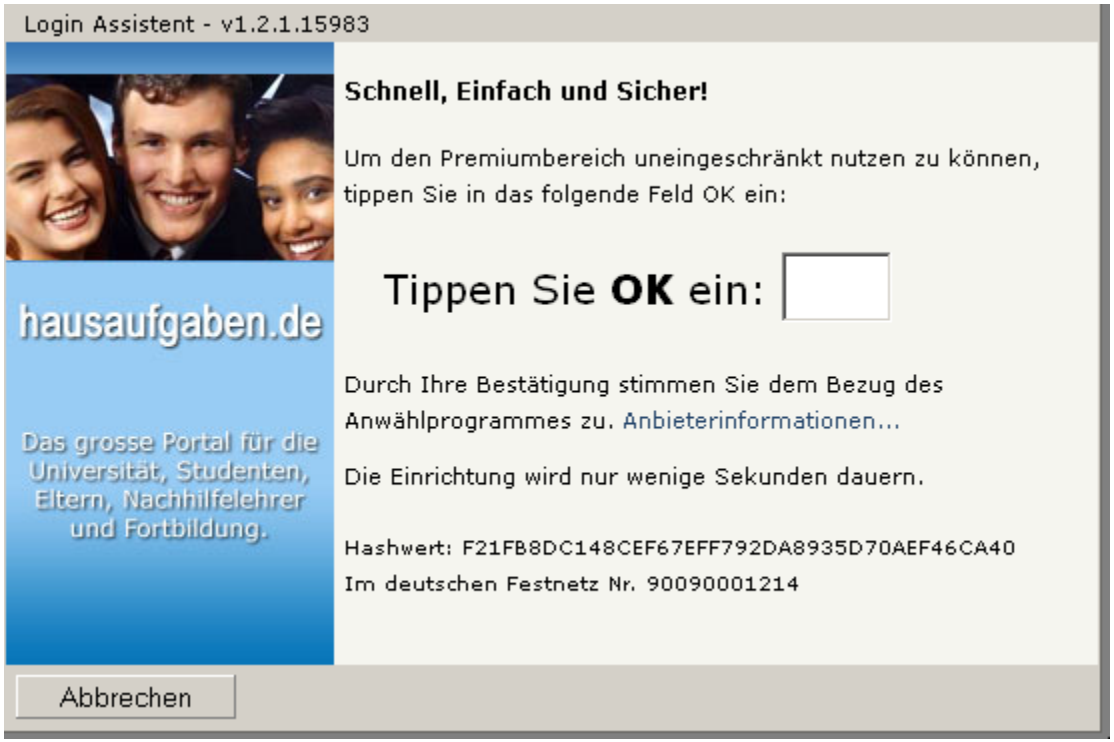
Name und Adresse:	Walter Temmer visions4tomorrow marketing GmbH Joesserstrasse 12 8430 Tillmitsch AT

Administrativer Ansprechpartner

Der administrative Ansprechpartner (admin-c) ist die vom Domaininhaber benannte natürliche Person, die als sein Bevollmächtigter berechtigt und gegenüber DENIC auch verpflichtet ist, sämtliche die Domain hausaufgaben.de betreffenden Angelegenheiten verbindlich zu entscheiden.

Name:	Manuel Schmidtlein
Kontakttyp:	PERSON
Adresse:	Vor der Hube 3
PLZ:	64572
Stadt:	Buettelborn
Land:	DE

Kostenpflichtige Internetangebote



Social-Engineering-Attacken

Als Social-Engineering wird das Auskundschaften von Benutzer und Firmendaten durch direkten Kontakt zu Mitarbeitern eines Unternehmens bezeichnet.

Als Methoden dienen

- Spurensuche im Web,

- direkte Kontaktaufnahme durch Chatprogramme, Internet Relay Chat oder Instant Messaging

➔ Ziel: Profiling

Sozial Engineering

Der gläserne Franzose

Einem französischen Internetnutzer ist der Spaß am Surfen vergangen, als er in einer Zeitschrift ein ausführliches Porträt über sich gelesen hat. "Ich habe sofort alle Angaben über mich im Internet gelöscht", sagte der Mann der französischen Tageszeitung "Presse Océan". Eine Zeitschrift hatte ihn im Dezember per Zufall herausgepickt, um einen Artikel über ihn zu schreiben - mit den Angaben, die der Mann selbst auf Websites wie Facebook, YouTube und Flickr über sich gemacht hatte. In dem Porträt ist über Familie und Ex-Freundinnen des Franzosen sowie über seine Arbeit und Hobbys zu lesen, selbst seine Handynummer wird genannt.

/Quelle: www.n-tv.de, 15.01.2009/

Computerbetrug

§263a des Strafgesetzbuches

„Wer in der Absicht, sich oder einem Dritten einen rechtswidrigen Vermögensvorteil zu verschaffen, das Vermögen eines anderen dadurch beschädigt, dass er das Ergebnis eines Datenverarbeitungsvorgangs durch unrichtige Gestaltung des Programms, durch Verwendung unrichtiger oder unvollständiger Daten, durch unbefugte Verwendung von Daten oder sonst durch unbefugte Einwirkung auf den Ablauf beeinflusst, wird mit Freiheitsstrafe bis zu 5 Jahren oder mit Geldstrafe bestraft.“

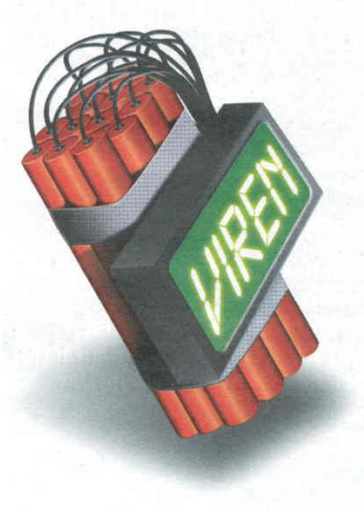
Schadprogramme – Piraten Software

„Früher war es eine Frage der Ehre, dass sich ein Virus möglichst weit verbreitete, um dann laut auf sich aufmerksam zu machen. Damit stillten die Programmierer ihr Geltungsbedürfnis. **Heute geht es nur noch ums Geld**.“

/c‘t 2007/2 Piratensoftware – wenn Schadprogramme des PC kapern/

Computerviren

(Fast) kein Virus aktiviert sich gänzlich ohne Ihre Hilfe.



Computerviren

ISS-Studie: Neun neue Computer-Schädlinge pro Tag
[19.11.2003 12:52]

Nach dem neuen IRIS-Report von **Internet Security Systems[1]** (ISS) tauchten insgesamt 823 neue Viren und Würmer im dritten Quartal 2003 auf. Damit stieg die Zahl der registrierten Schädlinge um satte 26 Prozent im Vergleich zum letzten Vierteljahr. Im Schnitt tauchten neun neue Schädlinge pro Tag auf.

IRIS-Report[2] für das 3. Quartal 2003 (PDF-Format)

https://gtoc.iss.net/documents/summaryreport.pdf

Malware

Malware (Malicious Software – bösartige Software) ist der Oberbegriff für eigenständige Programmtypen:

- **Viren** (klassische Form hat heute fast keine Bedeutung mehr)
- **Würmer**
- **Spyware und Adware**
- **Trojaner**
- **Backdoor**
- **Bots**
- **Spam**
- **Phishing**

Computerviren

Als Erfinder der Computerviren gilt F. Cohen, der 1983 erstmals mit derartigen Softwarepro-dukten experimentierte. Er definiert Viren wie folgt:

"Wir definieren einen Computer->>Virus<< als ein Programm, das andere Programme >>infizieren<< kann, indem es diese so modifiziert, daß sie eine eventuell modifizierte Form von ihm enthalten. Durch diese Eigenschaft zu infizieren, kann sich ein Virus in einem Com-puter oder Netzwerk ausbreiten, indem es die Autorisierungen der ihn aufrufenden Nutzer verwendet, um deren Programme zu infizieren. Jedes infizierte Programm kann sich ebenfalls wie ein Virus verhalten, wodurch sich die Infektion ausbreitet."

(Computer)viren - Meilensteine

- 1983 – F. Cohen erste Experimente mit Viren
- 1986 – der erste PC-Virus wird in Pakistan veröffentlicht
- 1988 – der erste Macintosh-Virus taucht auf
- 1989 – Der Trojaner AIDS verschlüsselt die Festplatte, Schlüsselherausgabe nur gegen Lösegeld.
- 1991 – Tequila – Virus als erstes polymorphes Virus
- 1992 – Michelangelo – Virus erstmals mit Medienschlagzeilen
- 1996 – Concept – Virus als erstes Macro-Virus für Word-Dokumente
- 1996 – Staog – Virus das erste Linux-Virus wird veröffentlicht
- 1998 – Back Orifice ist das erste Remote-Control-Trojanerprogramm
- 1999 – Melissa – Virus, das erste Virus, das sich per E-Mail verbreitet
- 2000 – Die ersten großangelegten Denial-of-Service Angriffe gegen Server
- 2000 – Timofonica Wurm, der erste Wurm, der Handys angreift
- 2000 – Life Stages-Wurm, der erste Wurm, der sich als SMS-verbreitet

Symptome einer aktuellen Vireninfektion

- **möglichst keine**
- ggf. Beeinträchtigung der Systemleistung
- Erhöhung der Onlinekosten
- Schadprogramme verschwinden spurlos
- beeinträchtigen die Funktion von Virenscannern
- entfernen selbst andere Schadprogramme

Klassische Ansteckungstechniken

Direkte Ansteckung – jedes Mal, wenn das infizierte Programm ausgeführt wird, werden eine oder mehrere Dateien infiziert.

Schnelle Ansteckung – Jede Datei, die von einem infizierten Programm angesprochen wird, wird verseucht.

Langsame Ansteckung – Das Virus steckt nur neue Dateien oder Dateien, die von einem nicht infizierten Programm geändert werden, an.

Inkonsistente Ansteckung – Das Virus befällt Dateien zufällig.

Speicherresidente Ansteckung – Jede Diskette und jedes auszuführende Programm wird infiziert.

Viren

Biologische Viren	Computerviren
Greifen spezielle Körperzellen an.	Greifen auf bestimmte Programme zu.
Die Erbinformationen einer Zelle werden verändert.	Das Programm wird manipuliert, es erfüllt andere Aufgaben als ursprünglich beabsichtigt.
In der befallenen Zelle wachsen neue Viren heran	Das befallene Programm produziert selbst Virenprogramme.
Eine infizierte Zelle wird nicht mehrfach vom gleichen Virus befallen.	Ein Programm wird von den meisten Viren nur einmal infiziert.
Ein befallener Organismus zeigt u.U. lange Zeit keine Krankheitserscheinungen.	Das infizierte Programm kann u.U. lange Zeit fehlerfrei weiterarbeiten.
Nicht alle Zellen, die mit dem Virus in Kontakt kommen, werden infiziert.	Programme können gegen bestimmte Viren immun gemacht werden.
Viren können mutieren und sind somit nicht immer eindeutig zu erkennen.	Virenprogramme können sich verändern und dadurch Suchprozeduren ausweichen.

Spyware und Adware

Auf dem Computer werden Programme installiert, die auf den ersten Blick harmlos erscheinen. Die Schadfunktion besteht darin, dass man eine Vielzahl Werbe-Pop-ups erhält bzw. der Computer wird ausspioniert. (Keylogger)

Trojanische Pferde

Trojanische Pferde (Trojaner) unterscheiden sich von Viren dadurch, dass sich der Code nicht repliziert.

Ein trojanisches Pferd ist ein Programm, welches vorgibt, eine nützliche Aktivität durchzuführen. Im Hintergrund wird ein Prozess gestartet, welches Daten auf dem Rechner ausspioniert oder Programme installiert, die anderen die Kontrolle über den Rechner geben.

Häufig werden trojanische Pferde mit elektronischen Glückwunschkarten oder Spaßprogrammen verteilt.

Schaden:

z.B. E-Mails unter falschen Namen versenden,

Internetverbindungen mit falschem Kennwort aufbauen

Trojaner - Industriespionage

Trojaner werden gezielt eingesetzt um gezielt Personen oder Unternehmen auszuspionieren. Programme werden gezielt in Unternehmensnetze eingeschleust um entsprechende Daten zu erhalten.

Beispiel England:
geknackte on-line-Bankig-Zugänge verursachen monatlich einen Schaden von über 3,5 Millionen Euro

/Quelle: CHIP-Heft 8/2005 S. 31/

Trojanische Pferde

Kaum ein Begriff wird so oft gegoogelt wie "Paris Hilton". Doch die Fans des It-Girls müssen vorsichtig sein, denn ihre Internetseite wurde von fiesen Hackern übernommen.

Der Hack wurde vom Sicherheitsdienstleister ScanSafe entlarvt, berichtet das US-Magazin PC World. Besucher von Parishilton.com werden von einem Pop-Up-Fenster aufgefordert, Software herunterzuladen, mit der die Seite besser dargestellt werden soll. Ganz egal ob die User "Yes" oder "No" klicken, versucht die verseuchte Seite den Trojaner Spy.Zbot.YETH herunterzuladen. Wird der Trojaner durch kein Schutzprogramm gestoppt, installiert er sich selbstständig auf dem Rechner des Besuchers und macht sich daran, Passwörter und andere geheime Daten auszuspäen. Außerdem versucht der ungebetene Gast, weitere Schädlinge nachzuladen.

/www.n-tv.de,
13.01.2008/

Botnet

Unter einem **Botnet** versteht man ein **fernsteuerbares Netzwerk von PCs,** welches aus untereinander kommunizierenden Bots besteht. Diese Kontrolle wird durch Viren bzw. Trojaner erreicht, die den Computer infizieren und dann auf Anweisungen warten, ohne auf dem infizierten Rechner Schaden anzurichten. Diese Netzwerke können für Spam-Verbreitung, DDoS Attacken, usw. verwendet werden, z.T. ohne dass die betroffenen PC-Nutzer etwas davon mitbekommen.

Unter einem **Bot** (angelehnt an *robot*) versteht man eine Klasse von Computerprogrammen, die weitgehend autonom solchen Aufgaben nachgehen, mit denen eine menschlich-interaktiv gesteuerte Software zeit- oder mengenmäßig überfordert wäre.

Ein Bot ist ein tendenziell eher simples, fleißiges „Arbeitswesen“. Ungebräuchlich ist die Bezeichnung daher für quasi-selbständige Programme im Bereich der Künstlichen Intelligenz.

/Quelle: www.wikipedia.de/

DDos-Attacke

Als **DoS**-Angriff (**Denial of Service** attack, etwa: *Dienstverweigerungs*-Angriff) bezeichnet man einen Angriff auf einen Host (Server) mit dem Ziel, einen oder mehrere seiner Dienste arbeitsunfähig zu machen. In der Regel geschieht das durch Überlastung. Erfolgt der Angriff koordiniert von einer größeren Anzahl anderer Systeme aus, so spricht man von einem **DDoS** (**Distributed Denial of Service**). Normalerweise werden solche Angriffe nicht per Hand sondern mit Backdoor-Programmen oder ähnlichem durchgeführt, welche sich von alleine auf anderen Rechnern im Netzwerk verbreiten, und dadurch dem Angreifer weitere Wirte zum Ausführen seiner Angriffe bringen.

Mit der Androhung derartiger DDoS-Atacken erpresst die Botnet-Mafia Schutzgelder!

/Quelle: www.wikipedia.de/

Bot-Net-Client

Bot-Net-Clients

- versenden Spam unter Kontrolle von außen,
- spionieren Daten aus,
- laden bezahlte Werbung oder
- legen durch verteilte Denial-of-Service-Atacken fremde Rechner lahm.

Diese Bot-Net-Clients werden zu großen Netzen zusammengeschaltet und vermietet.
besonders wertvoll: dedizierte Server bei Webhostern zur **Steuerung von Bot-Netzen** oder als **Server für Phishing-Sites**

Bot-Net-Client

Problem:

Wird der infizierte Computer für Straftaten missbraucht, hinterlässt er seine IP-Adresse als Spur, der die Ermittlungsbehörden folgen, um den Rechner ggf. zu beschlagnahmen.

Bot-Net-Client

Wer haftet für angerichtete Schäden?

Eindeutig **strafbar** macht sich, wer Schadprogramme **vorsätzlich freisetzt** (Computersabotage, Datenveränderung, Computerbetrug). Weiterhin drohen sehr hohe zivilrechtliche Schadensersatzforderungen.

Bei **unbewusster, vorsatzloser** Verbreitung von Malware ist ein Versender dann haftbar, wenn für ihn eine Pflicht zum Virenschutz besteht und er dieser nicht nachgekommen ist.

Für Privatpersonen gibt es keine expliziten gesetzlichen Vorgaben.

Würmer

Würmer sind eigenständige Programme, die sich über Sicherheitslücken in Netzwerkdiensten verbreiten. Sie werden häufig als E_Mail-Anhang versendet.

Phishing

Phishing ist eine Form des Trickbetruges mit Methoden des Social Engineerings. Es ist der Oberbegriff für illegale Versuche, weitgestreut Anwendern Zugangsdaten (Loginnamen plus Passwörter) für sicherheitsrelevante Bereiche zu entlocken. Phishing ist eine Variante des Identitätsdiebstahls. Rechtlich gesehen bewegen sich die Täter außerhalb der Legalität und sind oft der organisierten Kriminalität zuzuordnen.
Die Bezeichnung *Phishing* leitet sich vom Fischen (engl.: fishing) nach persönlichen Daten ab. Es könnte unter Umständen sein, dass der Ausdruck auch auf **p**assword **h**arvesting f**ishing** zurückführbar ist. Gängige Ziele von Phishing-Attacken sind Zugangsdaten für Banken (Onlinebanking), Versandhäuser, Internet-Auktionshäuser, webbasierende Onlineberatungen oder Kontaktportale. Durch anschließenden Mißbrauch der gestohlenen Zugangsdaten kann den Opfern viel Schaden zugefügt werden.

/Quelle: www.wikipedia.de/

Sicherheitsregeln für das Internet-surfen und den E-Mail-Verkehr

- Klicken Sie generell **niemals auf in E-Mails enthaltene Links**, sondern tippen Sie die Internetadressen gewünschter Seiten immer manuell ein!
- Schalten Sie die **Funktion "Aktive Inhalte ausführen" generell aus**. Wenn Sie darauf nicht verzichten wollen, so stellen Sie über die entsprechenden Funktion in den Sicherheitseinstellungen zumindest sicher, dass Ihr Browser in jedem Einzelfall bei Ihnen anfragt, ob Aktive Inhalte ausgeführt werden dürfen.

Quelle: www.bsi-fuer-buerger.de

Sicherheitsregeln für das Internet-surfen und den E-Mail-Verkehr

- Öffnen Sie E-Mails und darin enthaltene Anhänge nur dann, wenn Sie aus vertrauenswürdiger Quelle stammen.
- Setzen Sie eine **Firewall und Virenschutzsoftware** ein und bringen Sie diese regelmäßig auf den aktuellen Stand.
- Achten Sie darauf, dass Sie auch die **Softwareaktualisierungen** für Ihr Betriebssystem und andere von Ihnen eingesetzte Programme laufend installieren oder nutzen Sie automatische Update-Dienste.

Quelle: www.bsi-fuer-buerger.de

Phishing

Your mailbox has exceeded the storage limit set by your administrator. You may not be able to send or receive new mail until your mailbox size is increased by your system administrator. You are required to contact your system administrator through e-mail with your Username:{ } and Password:{ } to increase your storage limit.

System Administrator
E-mail: systemquota@live.com

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit.

This email is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged and confidential.

Phishing

Your mailbox has exceeded the storage limit set by your administrator. You may not be able to send or receive new mail until your mailbox size is increased by your system administrator. You are required to contact your system administrator through e-mail with your Username:{ } and Password:{ } to increase your storage limit.

System Administrator
E-mail: system-management1@live.com

You will continue to receive this warning message periodically if your inbox size continues to exceed its size limit.
This email is intended only for the use of the individual or entity to which it is addressed and contains information that is privileged and confidential.

Internet-Betrug

Dienstag, 29. Juni 2004
Groß angelegter Internet-Betrug
Fingierte Porno-Rechnungen

Die Hamburger Staatsanwaltschaft hat einen Fall von Internetkriminalität mit bis zu 30.000 Geschädigten aufgedeckt. Der Gewinn der Betrüger wird auf bis zu zwei Millionen Euro geschätzt, sagte der Leitende Oberstaatsanwalt Martin Köhnke am Dienstag in der Hansestadt.

"Die Haupttäter sitzen im Ausland, betreiben ihr Geschäft weltweit und kassieren unglaubliche Summen." Die Ermittler gehen davon aus, dass das Hamburger Unternehmen und eine weitere Firma insgesamt 150.000 Rechnungen verschickt haben.

Adresse:
http://www.n-tv.de/5259074.html

Internet-Betrug

Tausenden Internet-Surfern waren jeweils 69,95 Euro für den angeblichen Besuch von Web-Seiten mit erotischem Inhalt in Rechnung gestellt worden. Dabei stammten die Opfer aus allen Gesellschaftsschichten, auch ein Hamburger Rechtsanwalt sei angeschrieben worden.
Nach den Ermittlungen der Staatsanwaltschaft hatten die Betrüger einen so genannten Dialer eingesetzt, der die Telefonnummern von Internet-Surfern ausforschte. Clickten Surfer ein bestimmtes Werbebanner an, öffneten sich gleich mehrere Web-Seiten, die auch das Laden des Dialers bewirkten. Wenige Tage später erhielten die überraschten Surfer eine Rechnung für den einmonatigen Zugang zu einer Porno-Seite. Dabei fälschten die Betrüger auf technischem Wege Beweismittel, die die Polizei irreführten und den Eindruck erweckten, das Opfer habe sich tatsächlich in eine Porno-Seite eingewählt.

Adresse:
http://www.n-tv.de/5259074.html

Internet-Betrug

Guten Tag,
die Gesamtsumme für Ihre Rechnung im Monat Juni 2005 beträgt:
25566,53
Euro.
Mit dieser E-Mail erhalten Sie Ihre aktuelle Rechnung und - soweit von Ihnen beauftragt - die Einzelverbindungsübersicht.

Sind Sie Unternehmer und benötigen unsere Rechnung zur Geltendmachung von
Vorsteuerabzug? Bitte beachten Sie dann, dass Sie seit 29.12.2004 die Möglichkeit haben, Ihre Rechnung per E-Mail mit einer qualifizierten elektronischen Signatur zu erhalten. Sie können diese im Bereich "persönliche Einstellungen" aktivieren.

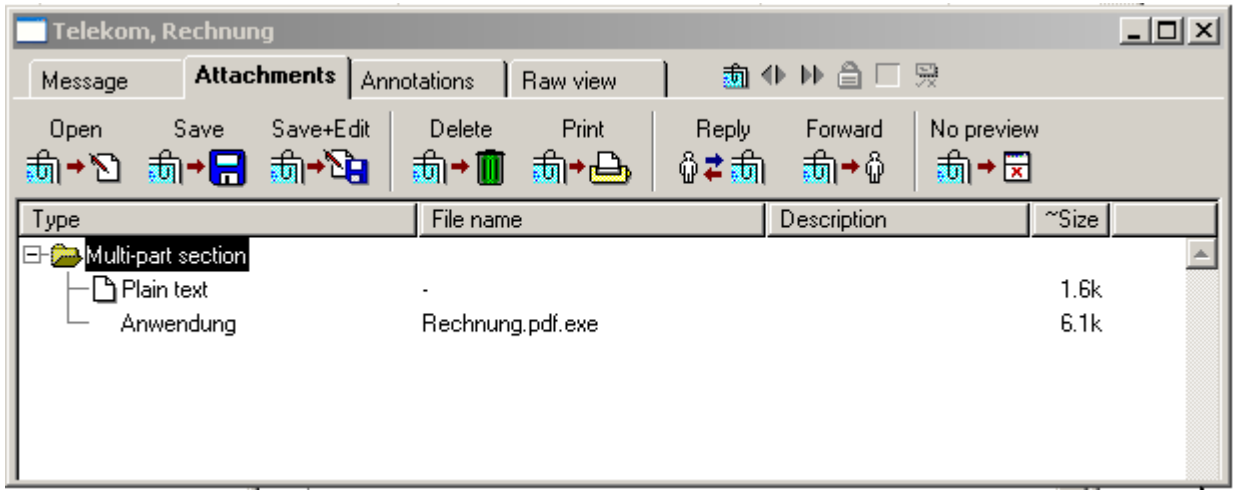
Internet-Betrug

Sollten Sie dem Finanzamt bisher eine von Ihnen zusätzlich beauftragte Rechnung in Papierform zum Vorsteuerabzug vorgelegt haben, bitten wir außerdem zu beachten, dass wir Ihnen diese nur noch in Form eines "Rechungsdoppels" bieten können, da nur so vermieden werden kann, dass T-Com mehrere Rechnungsoriginale ausstellt.

Antworten auf Ihre weiteren Fragen zur digitalen Signatur finden Sie auch in unseren FAQs unter dem Stichwort "Digitale Signatur".

==========
RECHNUNG ONLINE - TIPP DES MONATS
Die neuen WünschDirWas Tarife sind jetzt da! Jetzt online anmelden unter
www.t-com.de/reo/WuenschDirWas und bis zu 10,- Euro sparen.
Die aktuellen Top-Angebote der Deutschen Telekom finden Sie unter:
www.t-com.de/aktuell.
==========

Internet-Betrug



Malicious Code - Logische Bomben

Logische Bomben richten beim Start sofort Schaden an.

Mögliche Schadfunktionen sind das Löschen der Partitionstabelle oder das Überschreiben der IO.SYS.

Malicious Code - Spionageprogamme

Beispiel: Back Orifice

Das Programm besteht aus einem Back Orifice Server und einem Back Orifice Client. Wird die Glückwunschkarte aktiviert, so wird parallel der Server interaktionsfrei installiert. Von einem anderen Rechner kann jetzt mittels des Clients auf den infizierten Rechner zugegriffen werden.

Malicious Code - Hoaxes

Als Hoaxes (engl. hoax, altengl. hocus: Scherz, Falschmeldung) werden Falschmeldungen zu Computerviren bezeichnet. Häufig werden die Empfänger dieser Meldungen aufgefordert, sie an andere weiterzuschicken.

Schadfunktionen:

- Verunsicherung der Nutzer
- Erzeugen von nutzlosem Datenverkehr
- echte Viren als Attachement

Info: http://www.hoax-info.de/

Spam-Mail

E-Mail → E-Müll

weltweit werden täglich ca. 31 000 000 000 E-Mails verschickt

Spam-Mail

Spam-Mails werden häufig ohne Kenntnis von E-Mailadressen generiert. Eine Möglichkeit zur Verifizierung besteht darin, die Mail als Web-Seite zu gestalten und 1-Pixel-Bilder einzubinden, die nicht Bestandteil der Web-Seite sind, sondern von einem ftp-Server nachgeladen werden.

(Hotmail erkennt nach eigenen Angaben 2,4 Milliarden Spam-Mails täglich) /PC PROFESSINELL 9/2003/

(weltweit täglich ca. 31 000 000 000 E-Mails)

Spam-Mail

heise online: AOL blockierte 2003 eine halbe Billion Spam-Mails
[03.01.2004 14:29]
Der US-amerikanische Online-Dienst AOL[1] hat im vergangenen Jahr eine **halbe Billion E-Mails als Spam** identifiziert und aus dem Verkehr gezogen. Das geht aus einer Pressemitteilung[2] des Unternehmens hervor. Es lobt dabei die Mithilfe der Nutzer, die über den "Report Spam"-Knopf unerwünschte Nachrichten an das "AOL Postmaster Team" melden können. Auf jedes AOL-Mitglied zielten demnach im vergangenen Jahr durchschnittlich 15.000 unerwünschte Werbebotschaften. Etwa 75 bis 80 Prozent des täglichen Mail-Aufkommens würden herausgefiltert.

Spam-Mail

14.01.2007 14:58 **Identitätsdiebstahl mit erpresserischen Mails**
Anfang Dezember vergangenen Jahres kursierten E-Mails eines vermeintlichen Berufskillers durchs Netz, in denen der Empfänger dazu aufgefordert wurde, mehrere tausend US-Dollar an den Absender zu zahlen, sonst werde dieser den Empfänger töten. Wie aus einem Update der **Warnung** des **FBI** vor diesem makabren Betrugsversuch hervorgeht, treibt der Fall nun neue Blüten.
Es sollen weitere E-Mails aufgetaucht sein, die vorgeblich von der FBI-Dienststelle in London kommen. Darin soll zu lesen stehen, dass eine Person festgenommen wurde, die man in Zusammenhang mit den Droh-Mails wegen Mordes an mehreren Bürgern aus den USA und Großbritannien verdächtigt. Beim Verdächtigen seien Informationen gefunden worden, die auf den Empfänger der E-Mail an nächstes Opfer hinweisen. Der Empfänger solle daher umgehend Kontakt mit dem FBI in London aufnehmen, um bei den Ermittlungen mitzuhelfen. Offenbar wollen der oder die Absender so an persönliche Daten des Betroffenen gelangen, um Identitätsklau zu betreiben. Das (echte) FBI warnt eindringlich davor, auf die Forderungen des (falschen) FBI einzugehen. Sollte die Mail persönliche Information enthalten, die sie "vom üblichen Spam unterscheiden", sollte der Betroffene den Fall der Polizei melden.
Quelle: http://www.heise.de/newsticker/meldung/83677

Computerviren - Macroviren

Mit der Möglichkeit, an Dokumente (Textdateien) abarbeitungsfähige Programme zu koppeln, konnten auch diese Dateien von Computerviren befallen werden. Die an die Texte gekoppelten Dateien werden als Macros bezeichnet. Daher wird für die Viren der Begriff Macroviren verwendet. Mit der Version 6 des verbreiteten Textverarbeitungssystems WinWord wurde eine leistungsfähige Macro-Programmiersprache, das Word-Basic ausgeliefert. Aktuelle Word-Dokumente enthalten einige Funktionen, die sehr nützlich, aber auch sehr gefährlich sein können. Macroviren verändern und befallen u.a. die Vorlagendateien.

Aktuelle Macroviren werden auch mit VB-Script erstellt.

Computerviren - Macroviren

- Ein Dokument kann ein Macro enthalten, welches sofort beim Öffnen des Dokumentes ausgeführt wird.
- Ein Macro, einmal gestartet, kann Veränderungen in den globalen Macroeinstellungen vornehmen, so daß alle zukünftig bearbeiteten Dokumente mit diesen Änderungen versehen werden.
- Macros können Systemzugriffe realisieren.

Diese Viren haben in wenigen Jahren den größten Anteil an den Computerviren. Mit dem Austausch von Dokumenten, auch über das Internet, verbreiten sich diese Viren. Beim Öffnen eines Dokumentes werden die Makros abgearbeitet. Viele verändern die normal.dot (auch ein Schreibschutz wird von einigen Viren umgangen).

Die Schadfunktionen können bis zur Formatierung der Festplatte gehen.

Computerviren - Macroviren

Beispiel: Melissa

26.03.1999 (Fr) W97M_Melissa wird entdeckt

27.03.1999 (Sa) Erste Mailserver in Amerika sind überlastet/werden ausgeschaltet

28.03.1999 (So) Große Konzerne sind betroffen

29.03.1999 (Mo) Melissa ist bereits weltweit verbreitet, Mailserver in Europa werden abgeschaltet

30.03.1999 (Di) Erste Hinweise auf den Virusautor, über 100000 infizierte Systeme

31.03.1999 (Mi) FBI und AOL Spezialisten kreisen den Autor ein

02.04.1999 (Fr) David L. Smith wird als vermuteter Virenautor verhaftet

Computerviren - E-Mailviren

E-Mails werden als Transportmedium für Viren verwendet. Dabei treten zwei unterschiedliche Formen auf.

Viren als Mail-Attachement:
Beispiel: Internet Wurm Bad Ass (BadAss.exe)
Wird der Wurm durch Start der Datei aktiviert, so durchsucht er die Outlook-Adressbücher und verschickt sich als E-Mail an die gefundenen Adressen („Did is well grapping“)

Viren in einer Mail:
Beispiel: Internet-Wurm Bubble-Boy
Beim Öffnen erzeugt das Skript die Datei UPDATE.HTA. Die Wirkungsweise ist analog zu Bad Ass. Er verschickt sich selbst als Mail an die gefundenen Adressen („Bubbleboy is back“)

Computerviren – Gegenmaßnahmen

Kein Antivirenprogramm bietet 100% Schutz!

aber:
Gesundes Misstrauen gegenüber Dateien, die per E-Mail ankommen, ist ein guter Schutz.

Kontrollfragen

1. Erklären Sie die Begriffe Datenschutz und Datensicherheit. Nennen Sie die gesetzliche Grundlage für den Umgang mit personenbezogenen Daten in Deutschland und deren grundlegenden Zweck. Welche Auswirkungen haben diese Gesetze auf den Umgang mit personenbezogenen Daten in der Schule und Ausbildung?
2. Nennen Sie die Schwerpunkte des Informations- und Kommunikations-Dienste-Gesetzes. Welche Verantwortung leitet sich aus diesem Gesetz bei der Erstellung und Präsentation von Internetseiten ab? Welche weiteren Gesetze sind bei der Präsentation von Informationen im Internet zu beachten?

Kontrollfragen

3. Erläutern Sie den Begriff Malware (Malicious Software – bösartige Software). Klassifizieren Sie vier typische Programmtypen für Malware und beschreiben Sie kurz deren Wirkungsweise.
4. Erläutern Sie den Begriff Computervirus und beschreiben Sie die Wirkungsweise. Vergleichen Sie Computerviren mit biologischen Viren. Nennen Sie heute typische Verbreitungswege für Computerviren. Welche Maßnahmen können Sie zum Schutz eines Schulcomputerlabors vor Computerviren ergreifen?