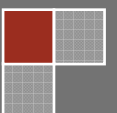




@

# Internet-Kriminalität

Methoden, Schutz und Gesetze im und ums Internet.



# Inhaltsverzeichnis

---

1.	Motivation.....	4
2.	Formen der Internet-Kriminalität .....	5
2.1.	Thematische Formen.....	5
2.1.1.	Harte Pornografie.....	5
2.1.1.1.	Kinderpornografie .....	5
2.1.1.2.	Tierpornografie / Gewalttätige-Pornografie.....	5
2.1.1.3.	Zugänglichkeit der Internet- Sexualität .....	5
2.1.2.	Urheberrechtsverletzungen .....	5
2.1.3.	Gewaltdarstellungen, Extremismus, Rassismus .....	5
2.1.4.	Social Engineering / Social Hacking .....	6
2.1.4.1.	Phishing, Hijacking.....	6
2.1.4.2.	Vishing, Phreaking .....	6
2.1.4.3.	Hoaxes .....	6
2.2.	Technische Formen .....	7
2.2.1.	Ansteckende Malware.....	7
2.2.1.1.	Viren .....	7
2.2.1.2.	Würmer .....	7
2.2.2.	Verborgene Malware.....	8
2.2.2.1.	Trojanisches Pferd .....	8
2.2.2.2.	Backdoor.....	8
2.2.2.3.	Rootkit .....	8
2.2.3.	Profitable Malware (Gray-Ware).....	9
2.2.3.1.	Spam, Junk, Spom.....	9
2.2.3.2.	Dialer .....	9
2.2.3.3.	Spyware .....	9
2.2.3.4.	Adware .....	9
2.2.3.5.	Logger .....	9
3.	Sicherer Umgang mit dem Internet .....	10
3.1.	Menschliche Vorsichtsmassnahmen .....	10
3.2.	Maschinellem Schutz.....	11
3.2.1.	Betriebssysteme .....	11

3.2.1.1.	Internet Zugriffsmöglichkeiten.....	11
3.2.1.2.	Anti-Viren Programme.....	12
3.2.1.3.	Anti-Spyware, Anti-Adware Programme .....	12
3.2.2.	Anti-Spam, Anti-Junk Programme .....	12
3.2.3.	Firewallsysteme.....	13
4.	Gesetze in der Schweiz.....	14
4.1.	Rechtliche Lage.....	14
4.1.1.	Onlinerecht.....	14
4.1.1.1.	Datenmissbrauch.....	14
4.1.1.2.	E-Banking .....	14
4.1.1.3.	Geldwäscherei .....	14
4.1.1.4.	Jugendlicher Hacker .....	15
4.1.1.5.	Tauschbörsen .....	15
4.1.1.6.	Texte kopieren.....	15
4.1.2.	Grauzonen .....	15
4.1.2.1.	E-Commerce Gesetz .....	15
4.1.2.2.	Urheberrecht.....	15
4.2.	Illegalitätsbekämpfung.....	16
5.	Interview mit Spezialisten.....	17
5.1.	Schaffhauser Polizei, Beat Schaffitz.....	17
5.2.	Internetspezialist, David Wagner .....	18
6.	Schlusswort .....	20
7.	Quellen.....	21
7.1.	Formen der Internet-Kriminalität.....	21
7.2.	Sicherer Umgang mit dem Internet.....	21
7.3.	Gesetze in der Schweiz.....	21
8.	Kontakt.....	22

# 1. Motivation

---

Diese Arbeit informiert über die Kriminalität im Internet. Es werden Formen der Kriminalität untersucht und mögliche Schutzmechanismen aufgezeigt. Auch der Rechtsschutz, die Legalität und die Rechte vom Schweizergesetzgeber im Internet werden untersucht.

Das Internet, ein Netzwerk welches heute nicht mehr wegzudenken ist. In diesem ist fast alles möglich. Leider wird das Internet oft auch als straffreier Raum angesehen. Immer mehr Benutzer werden wissentlich oder unwissentlich kriminell im Internet. Durch intelligente Software kann auch ein völlig harmloser Computer unwissentlich zu einem Schädling mutieren. Ich versuche mit dieser Arbeit auf die Gefahren im Internet hinzuweisen. Mein Ziel ist es, einem Laien welcher nur sehr wenig mit dem Internet in Berührung kommt, aufzuzeigen welche Gefahren und Schutzmöglichkeiten bestehen. Gleichzeitig möchte ich die Arbeit spannend für einen professionellen Internet Anwender gestalten, indem ich die Möglichkeiten der Internet Gefahren strukturiere und die engen Zusammenhänge aufzeige. Der Aufenthalt im Internet ist meiner Meinung nach nicht gefährlich. Durch das Beachten einiger Hinweise ist die Verwendung problemlos und die Berührung der Internet-Kriminalität niedrig. Ich liefere mit dieser Arbeit die notwendigen Hinweise.

Im ersten Teil ist es wichtig, dass einem Internet Benutzer die Gefahren aufgezeigt werden. Daher fasse ich Anfangs der Arbeit, alle Internet-Kriminellen Themen auf. Ich erkläre sie kurz, denn mit dem Wissen der Möglichkeiten, steigt auch die Selbstsicherheit eines Internet-Benutzers.

Im zweiten Teil möchte ich die Schutzmöglichkeiten aufzeigen, welche sehr wichtig sind. Viele Internet-Benutzer verstehen leider sehr wenig vom Internet-Schutz. Dies trägt dazu bei, dass die Internet-Kriminalität unwissentlich der Benutzer steigen kann.

Im dritten Teil, komme ich auf die Gesetze in der Schweiz zu sprechen. Ich werde einige realistische Fälle aufzeigen und die Wirkungen für den Betroffenen demonstrieren. Die Meinung eines Sicherheitsexperten welcher in einer Providerfirma arbeitet wird ebenfalls angefragt. Er beantwortet sicherheitsbezogene Fragen und gibt Tipps zur Sicherung des eigenen Computers. Spannende Antworten liefert auch die Polizei im Interview über Internet-Kriminalität.

## 2. Formen der Internet-Kriminalität

---

### 2.1. Thematische Formen

Ich strukturiere die Formen der Internet-Kriminalität in verschiedene Bereiche. In den thematischen Formen werden verschiedenste menschlich ausgelöste Straftaten aufgezeigt.

#### 2.1.1. Harte Pornografie

Sexualität ist im Internet weit verbreitet. Wahrscheinlich liegt dies an dem scheinbaren rechtsfreien und anonymen Raum. Kriminalität im Internet, in Zusammenhang mit Pornografie beinhaltet Kinderpornografie, Tierpornografie / Gewalttätige-Pornografie und die Zugänglichkeit der Internet-Sexualität.

##### 2.1.1.1. Kinderpornografie

Kinderpornografie bezeichnet Sexuelle-Gewalt an Kindern. Verstöße gegen das Gesetz werden mit hohen Strafen sanktioniert. Leider ist das Internet ein idealer Raum, um solchen Inhalt anonym zu verbreiten. Viele Organisationen auf der Welt versuchen dies zu verhindern, dennoch existieren Untergrund-Netzwerke welche Informationen dieser Art untereinander austauschen.

##### 2.1.1.2. Tierpornografie / Gewalttätige-Pornografie

Sexuelle Handlungen mit oder an Tieren sind ebenfalls verbotene Straftaten. Pornografie mit Gewaltdarstellungen, Bedrohungen oder Missbräuchen in elektronischer Form werden nicht toleriert und bestraft.

##### 2.1.1.3. Zugänglichkeit der Internet- Sexualität

Die im Internet angebotenen sexuellen Inhalte benötigen Zugriffsschutz für Minderjährige. Dieser Zugriffsschutz wird von vielen Sex-Anbietern nicht ernst genommen. Daher versuchen Organisationen, Institute und nicht zuletzt Länder auf die Gefahr der leicht bekömmlichen Inhalte im Internet hinzuweisen.

#### 2.1.2. Urheberrechtsverletzungen

Urheberrechtsverletzung ist ein Verstoss gegen das Urheberrecht. Dieser Verstoss wird durch das Erstellen einer unerlaubten Kopie eines Urheber geschützten Objektes gültig.

Urheberrechtsverletzende elektronische Medien werden oft auch als Raubkopie oder Schwarzkopie bezeichnet. Unter diesem Punkt machen sich sehr viele Internetnutzer strafbar. Zum Beispiel, eine durch einen Vertrieb vermarktete Musik CD-Rom entgegen einer Bezahlung herunterladen und zu verwenden ist eine Straftat.

#### 2.1.3. Gewaltdarstellungen, Extremismus, Rassismus

Gewaltdarstellung beschreibt Informationen welche grausame oder unmenschliche Verherrlichung oder Verharmlosungen beinhalten. Auch Rassismus oder Extremismus wird im Internet nicht geduldet. Das Problem gerade bei Rassismus ist, die Unabhängigkeit des Internets.

### 2.1.4. Social Engineering / Social Hacking

Social Engineering bedeutet auf Deutsch soziale Manipulation. Angreifer spionieren das Umfeld eines Opfers aus und erfahren durch gefälschte Identität geheime Informationen welche meist für das Eindringen in einen Computer verwendet werden. Man spricht beim Eindringen in einen Computer vom Social Hacking, wenn die Daten durch Social Engineering beschaffen wurden.

#### 2.1.4.1. Phishing, Hijacking

Phishing (Angeln) und Hijacking (Entführung, Diebstahl) sind eng verwandte Begriffe im Zusammenhang mit der Internet-Kriminalität. Es geht hauptsächlich um das Erlangen von Daten eines Internet Benutzers. Zum Beispiel wird ein Benutzer per Email aufgefordert sein Ebanking Passwort zu ändern. Mit der im Email angehängten möglichst gleichen Ebanking-Web-Adresse verbindet sich der Benutzer mit einer Website (URL-Hijacking). Darauf wird eine möglichst genaue Kopie der Originalen Bank-Seite hinter der Adresse abgebildet. Der Benutzer vermutet sich am richtigen Ort und könne sein Kennwort ändern. Mit Eingabe seiner Daten auf der gefälschten Internet Seite werden diese direkt dem Täter übergeben. (Phishing).

Hijacking trifft man noch in weiteren Situationen an. Browser-Hijacking, Network-Hijacking, TCP-Hijacking, Suchmaschinen-Hijacking.

#### 2.1.4.2. Vishing, Phreaking

Vishing ist ebenfalls eine sehr ähnliche Betrugsmethode. Diese wird jedoch bei der Internet Telefonie angewandt (VOIP). Zum Beispiel wird mit automatisierten Telefonanrufen die Irritierung des Empfängers erhofft, damit dieser geheime Zugangsdaten, Passwörter oder Kreditkartennummern herausgibt.

#### 2.1.4.3. Hoaxes

Das englische Wort Hoax bedeutet übersetzt schlechter Scherz. Es werden Meldungen meistens per Email oder Instant-Messaging (Chat-Systeme) verbreitet welche erschrecken sollen. Ein Hoax ist vergleichbar mit einem Aprilscherz, in welchem meistens nur Teilinformationen über die Verfasser hinterlegt sind.

## 2.2. Technische Formen

Internet-Kriminalität ist oft auch in Programmen anzutreffen. Das englische Wort Malware ist der Überbegriff für Programme oder Code, welcher sich unerwünscht, meistens selbständig in Software auf dem Computer einschleust. Die Bezeichnung Malware entstand aus den englischen Begriffen malicious „böartig“ und Software.

Malware wird in verschiedene Teile aufgeteilt.

### 2.2.1. Ansteckende Malware

Ansteckende Malware beschreibt böartige Software, welche sich selbst verbreitet. Unterschieden wird zwischen Viren und Würmern.

#### 2.2.1.1. Viren

Der Computervirus ist die älteste Variante von Malware. Der Virus wird anfänglich vom Menschen geschrieben. Der Schadcode verbreitet sich danach selbständig. Wird der Virus einmal vom Anwender gestartet, können sämtliche Funktionen der Computersoftware verändert werden. Man unterscheidet generell zwischen verschiedenen Arten von Computerviren.

Programmiviren, Systemviren, Makroviren, Scriptviren, Polymorphe Viren, Stealth-Viren, Hybridviren

#### 2.2.1.2. Würmer

Würmer sind eng verwandt mit Viren. Ein Virus wird vom Benutzer ausgeführt und somit in die Software eingefügt. Würmer hingegen versuchen sich selbst über das Internet zu verbreiten. Ein Wurm benötigt also eine Sicherheitslücke in einer Applikation oder in einem Betriebssystem. Wird der Wurm einmal auf einem Computer ausgeführt, scannt dieser andere Netzwerke nach möglichen Schwachstellen ab. Wird eine Schwachstelle entdeckt, versendet sich der Wurm von selbst und versucht sich im unsicheren System einzunisten. Danach werden von diesem neu-infizierten System weitere Würmer an andere Netzwerkbenutzer versendet.

Irrtümlich werden Würmer oft mit Viren verwechselt. Ein Wurm ist nach der Freisetzung in einem Netzwerk selbstständig. Ein Virus dagegen muss über einen Träger transportiert werden, so hängt dieser sich an eine Datei, welche durch Computernutzer unwissentlich weitergegeben wird.

### 2.2.2. Verborgene Malware

Verborgene Malware ist bösartige Software welche der Benutzer selbst nicht bemerkt. Auch hier gibt es verschiedene technische Ansätze wie zum Beispiel das Trojanische Pferd.

#### 2.2.2.1. Trojanisches Pferd

Ein Trojanisches Pferd beschreibt ein Computerprogramm welches beim Anwender als nützlich getarnte Software erscheint, jedoch im Hintergrund beliebige Funktionen ausführen kann. Damit dies funktioniert wird ein Trojanisches Pferd meistens in ein Scheinprogramm integriert. Vom Interesse gepackt öffnet der unschuldige Anwender die Software und installiert sich somit den Schädling auf sein System. Das getarnte Softwarestück installiert eine Backdoor Funktion, welche im nächsten Absatz genauer erläutert wird. Das Trojanische Pferd schleust selbst keinen Schädlichen Code in das System ein, sondern installiert Backdoor Programme. Wird das Trojanische Pferd auf dem System entdeckt und entfernt, ist mit Viren und Würmer zu rechnen.

Hier einige Tarnmethoden eines Trojaners:

Viele Trojaner bestehen aus zwei ausführbaren Dateien in einem Programm. Wird die einzelne Datei angeklickt öffnet diese ein Scheinprogramm wie auch getarnte Schadsoftware. Es gibt aber auch sinnvolle Software welche in sich selbst, vor dem Benutzer versteckt, ein Trojanisches Pferd beherbergt.

#### 2.2.2.2. Backdoor

Als Backdoor wird ein Programm beschrieben, welches einem nicht autorisiertem Benutzer Zugriff zu einem gesicherten System erlaubt. Eine Backdoor Software wird meistens über ein Trojanisches Pferd oder einen Wurm installiert.

Das Backdoor Programm ist nicht mit dem Trojanisches Pferd zu verwechseln. Das Trojanische Pferd ist eine Möglichkeit, Software unbemerkt zu implementieren. Eine Backdoor Software ermöglicht den Zugriff auf das System.

Über eine Backdoor Software können beinahe unbegrenzte Manipulationen eines Systems stattfinden.

#### 2.2.2.3. Rootkit

Ein Rootkit beinhaltet mehrere Softwarewerkzeuge welche erst nach einem Einbruch in ein Computersystem über einen Wurm oder Trojaner installiert werden. Die Werkzeuge versuchen Malware vor einem Benutzer, dem System und Programmen zu verbergen.

Häufigste Anwendung eines Rootkits ist das verstecken von sämtlicher Malware vor einem Antivirenprogramm. Es gibt einige Varianten von Root-Kits: Application-Rootkit, Kernel-, Userland-Rootkits, Speicher-Rootkits, Virtual-Machine-Rootkits

### 2.2.3. Profitable Malware (Gray-Ware)

Auch mit Malware ist das Geldverdienen möglich, daher existieren Methoden welche auf Profit zielen. Diese Methoden werden auch als Gray-Ware bezeichnet, da sie die grundsätzliche System Funktionalität nicht beeinflusst. So wird zum Beispiel in ein gekauftes Programm Werbung eingebaut. Klickt der Benutzer auf die Werbung, verdient der Werbeflächen-Anbieter Geld.

#### 2.2.3.1. Spam, Junk, Spom

Spam beschreibt eine Informationsflut welche vom Anwender nicht erwünscht ist. Es gibt viele verschiedene Spam Methoden. Die bekannteste Methode ist Email-Spam. Weitere Spam Methoden: Multi User Dungeons Spam, Usenet-Spam, Index-, Link-, Blog- und Wikispam, Spam over Mobile Phone (SPOM)

#### 2.2.3.2. Dialer

Ein Dialer ist eine Software welche immer mehr von der Oberfläche verschwindet. Sie wird verwendet um bei Einwählverbindungen eine andere Anschlussnummer zu wählen. Der Benutzer kann dadurch abgehört oder mit hohen Kosten belastet werden.

#### 2.2.3.3. Spyware

Spyware ermittelt das Verhalten des Benutzers und sendet die Daten an Dritte weiter. Oft wird solche Software für Marktforschung verwendet. Eine Firma kann zum Beispiel anhand von Spyware genau feststellen welche Webseiten von einem Benutzer besucht werden.

#### 2.2.3.4. Adware

Adware werden Programme oder Funktionen genannt, welche dem Benutzer ohne nachzufragen Werbung anzeigen. In einigen Fällen dient auch Adware zur Marktforschung. In einigen Fällen ist eine Malware Klassifizierung je nach Programm notwendig, da Spyware und Adware ein sehr ähnliches Verhalten aufbringen.

#### 2.2.3.5. Logger

Ein Logger ist ein Programm welches meistens versteckt im System funktioniert. Ein sogenannter Key-Logger zeichnet alle Eingaben über die Tastatur auf. Diese Eingaben können danach durch einen Angreifer nach nützlichen Informationen durchsucht werden. Somit wären vom Benutzer eingegeben Kennwörter leicht herauszufinden.

## 3. Sicherer Umgang mit dem Internet

---

### 3.1. Menschliche Vorsichtsmassnahmen

Viele kennen das Internet als so genanntes WWW (World Wide Web) in dem man mit einem Webbrowser auf Seiten herum surft und mit einem Email Programm Nachrichten versendet. Technisch gesehen ist das Internet mehr als nur ein Webbrowser oder ein Email System. Das Internet ist ein riesiges Netzwerk welches Computersysteme verbindet. Zum Beispiel könnte auf einem Hochverschlüsseltem Tunnel geheime Daten von Ort A nach Ort B übertragen werden, ohne das die Daten von einer unautorisierten Person je einmal gesehen werden. Daher ist im Internet der menschliche Verstand wichtig. Wie im realen Leben sollte auch im Internet nicht einfach alles ausprobiert werden, obwohl es technisch vielleicht möglich wäre. Wer dies doch tut, macht meistens Bekanntschaft mit der Internet-Kriminalität.

Malware Programme im Internet werden trotzdem häufig über Internet Webseiten oder Email Systeme übertragen. Wichtig ist daher, die richtigen Vorsichtsmassnahmen zu treffen damit das infizieren nicht möglich ist.

Wenn die Strassen im Winter vereist sind, fährt ganz sicher niemand schneller, als es die Höchstgeschwindigkeit vorschreibt. Wer einen Computer besitzt sucht nicht im Internet extra nach illegalen Seiten oder Grauzonen, auch wenn dies wegen der Anonymität verlockend ist. Den gerade bei solchen Aktionen ist der Computer sehr schnell von Malware Programmen infiziert. Somit wird der Benutzer selbst zu einem Internet Kriminalist.

Es ist generell Vorsicht geboten. Emails welche nicht bekannt sind, sollten nur mit grosser Vorsicht geöffnet werden (Email zuerst durch Virenschutz überprüfen). Unbekannte Internet-Seiten sollten möglichst nicht besucht werden. Wer trotzdem auf verschiedensten Ebenen herum surft, sollte unbedingt seine Software auf dem neusten und sichersten Stand halten. Dazu erkläre ich mehr unter maschineller Schutz.

### 3.2. Maschinelles Schutz

Natürlich kann es in seltenen Fällen vorkommen, dass auch einmal ein vertrauenswürdige Ziel im Internet verseucht ist. Daher trägt gerade der Zustand des Computers viel zum Schutz bei. Es gibt verschiedene Möglichkeiten, welche den Computer besser absichern:

#### 3.2.1. Betriebssysteme

Die Wahl des richtigen Betriebssystems ist sehr entscheidend. Grössere Verbreitung des Systems heisst auch mehr Risiken und Sicherheitslöcher. Daher ist jemand der ein wenig verbreitetes Betriebssystem verwendet automatisch besser geschützt. Der Aufbau des Benutzerrechtensystems ist ebenfalls wichtig. Ein Benutzer sollte nicht mit Vollrechten auf dem Computer arbeiten und im Internet surfen, da sich Malware aufgrund der Vollberechtigung einfach unterbringen kann. Es sollte auf jeden Fall darauf geachtet werden, dass der Computerbenutzer nur eingeschränkte Rechte besitzt, somit kann sich ein Virus nicht direkt ins System sondern nur in die Benutzerumgebung installieren und ist weit ungefährlicher.

Momentan sind ca. 80 % der Internet Benutzer Microsoft Windows Rechner. Die restlichen 20% sind Mac, Linux, Unix und verschiedene weitere Betriebssysteme. Daher ist klar das Microsoft Windows am meisten angegriffen wird. Lange Zeit gab es gar keine Malware für Linux, Unix oder Mac, inzwischen sind auch diese Betriebssysteme von Malware betroffen.

##### 3.2.1.1. Internet Zugriffsmöglichkeiten

Der Zugriff auf das Internet wegen Emails oder Informations-Seiten wird am meisten gebraucht. Die Wahl des Zugriffsprogramms auf Emails und Webseiten spielt dabei eine wichtige Rolle. Intelligente Programme erkennen Malware auf Webseiten oder in Email Nachrichten und blockieren diese (Das Löschen wird darauf meistens von Anti-Viren oder Anti-Spam Programmen übernommen). Die gleichen Regeln wie für Betriebssysteme, gelten für diese Programme. Jedoch kommt hinzu, dass sich Microsoft mit dem Internet Explorer lange Zeit nicht sonderlich Mühe gegeben hatte. Daher ist dies einer der unsichersten Internet Browser. Der Internet Explorer ist der Marktführer unter den Browsern wie auf der Grafik zu erkennen ist.

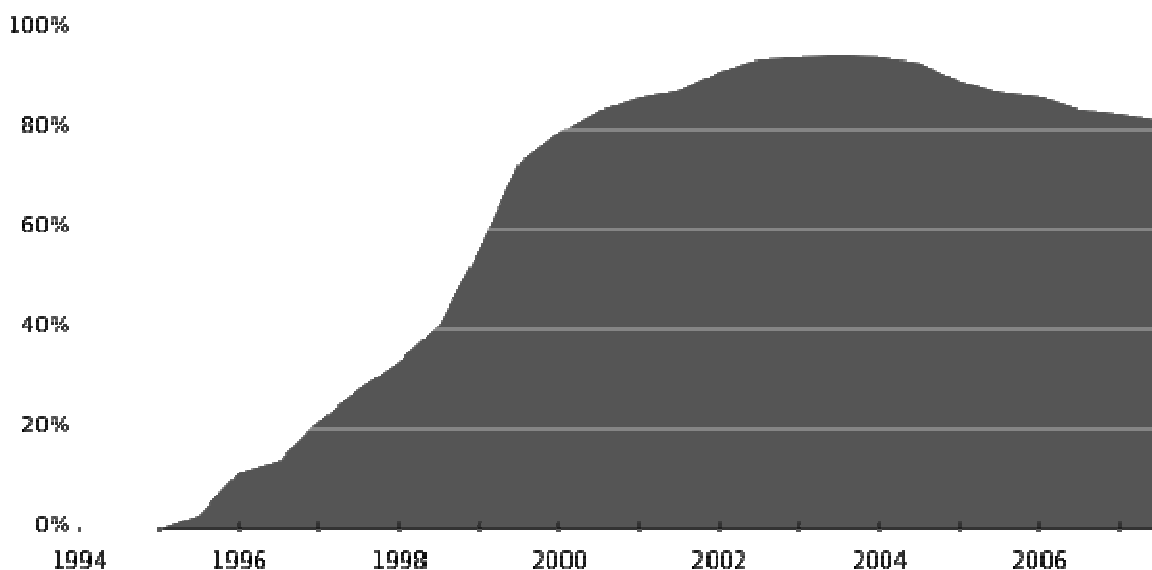


Abbildung 1: Microsoft Internet Explorer prozentuale Verbreitung

(Quelle: <http://upload.wikimedia.org/wikipedia/commons/c/ce/Internet-explorer-usage-data.svg>)

Der Internet Explorer ist bei den Windows Betriebssystemen von Anfang an mitgeliefert. Für Dritthersteller war es sehr schwierig ihre eigene Software neben dem Internet Explorer zu verbreiten. Aufgrund der schlechten Sicherheit des Internet Explorers haben sich inzwischen andere Browser Marktanteile erobert. Firefox und Opera sind seit dem Jahr 2007 weitverbreitet Internet Browser. Es sollte jedenfalls dringend darauf geachtet werden, dass der Internet Browser und das Email Programm auf dem aktuellsten Stand gehalten wird. Noch mehr Sicherheit bringt einen weniger verbreiteten Browser zu surfen.

Der Email Client ist nicht so enorm von direkten Angriffen betroffen. Dafür ist hier grosse Vorsicht bei den empfangenen Mails wichtig. Es sollten keine unbekanntes Mails geöffnet werden. Schnell ist Malware in einem Email versteckt und der Computer infiziert.

#### 3.2.1.2. Anti-Viren Programme

Anti-Viren Programme gibt es auf verschiedenen Ebenen. Sie dienen vor allem der Abwehr von Malware. Anfangs wurden Anti-Viren Programme gegen Viren und Würmer eingesetzt. Inzwischen versuchen modernere Programme alle Malware Methoden zu erkennen. Die Grenze zwischen Anti-Viren und Anti-Spyware Programmen ist je nach Hersteller fließend. Die meisten Anti-Viren Programme funktionieren direkt auf einem Betriebssystem und schützen dieses vor Malware. Eine Vielzahl der verschiedenen Anti-Viren Programme funktionieren unter Windows. Linux, Unix oder OSX (Mac) sind weniger von Malware befallen, daher gibt es für diese Plattformen weniger Anti-Viren Programme.

Anti-Viren Programme werden immer häufiger bei Email-Servern eingesetzt. Diese durchsuchen den Emailverkehr auf Malware.

#### 3.2.1.3. Anti-Spyware, Anti-Adware Programme

Anti-Spyware und Anti-Adware Programme durchsuchen Computer-Systeme nach Spyware oder Adware. Einige Anti-Viren Programme beinhalten diese Funktionen ebenfalls. Meistens werden Spyware und Adware Schutzmechanismen im gleichen Programm angeboten.

#### 3.2.2. Anti-Spam, Anti-Junk Programme

Ein Anti-Spam Programm wird meistens auf den Email-Client installiert, also dem lokalen Computer. Dieses filtert unerwünschte Emails aus dem Postfach. Meistens werden die Emails dann in einen speziellen „Spam“ oder „Junk“ Ordner verschoben, damit der Benutzer die Emails nochmals kontrollieren kann. Das manuelle kontrollieren durch den Benutzer ist zu empfehlen, da die Computer-Systeme nicht alle Nachrichten richtig filtern. Je nach Inhalt eines Emails kann auch ein vertrauenswürdiger Absender als Spammer gekennzeichnet werden.

Es gibt allerdings auch Anti-Spam Programme für E-Mail Server. Das Programm funktioniert dann direkt auf dem Server und der Benutzer merkt nichts von der Mailkontrolle. Es gibt verschiedene Möglichkeiten der Filterung eines Spam-Emails auf einem Server. Je nach Kundenwunsch kann das Email direkt auf dem Emailserver gelöscht werden oder mit einem Schriftzug „Spam“ gekennzeichnet werden und zum Benutzer weitergeschickt werden.

### 3.2.3. Firewallsysteme

Es gibt bei Firewallsystemen generell zwei Unterscheidungen. Die erste Möglichkeit ist eine Firewall direkt auf einem Arbeitscomputer zu verwenden. Man spricht in diesem Fall auch von einer Software Firewall. Die zweite Möglichkeit wäre eine Firewall vorzuschalten. Diese ist in den meisten Fällen eine Software, welche direkt auf angepasster Hardware funktioniert. Die dann sogenannte Hardware Firewall oder auch dedizierte Firewall kann die Grösse eines kleinen Kasten bis zu einem grossen Computer haben.

Auch Private Internetanwender sollten unbedingt die Vorteile einer Hardwarefirewall nutzen. Da eine Software-Firewall direkt auf dem Arbeitscomputer installiert ist, kann diese keinen so guten Schutz wie eine Hardware-Firewall bieten. Dies kann zu grossen Sicherheitslücken führen. Leider ist es bereits vorgekommen, dass anhand von Sicherheitslücken in Software-Firewalls Computer gehackt wurden. Eine Hardware-Firewall hingegen ist dediziert für das Abblocken von nicht erwünschtem Internet-Verkehr. Diese kann auch für mehrere Computer gleichzeitig verwendet werden und bietet auf jedenfall bessere Sicherheit als eines Software-Firewall.



Abbildung 2: dedizierte Firewall Systeme der Firma Watchguard  
(Quelle: [hardware4less.net.au/images/watchguard.jpg](http://hardware4less.net.au/images/watchguard.jpg))

## 4. Gesetze in der Schweiz

---

### 4.1. Rechtliche Lage

Leider gibt es in der Schweiz nicht einfach eine Plattform welche über die Gesetzte im Internet informiert. Da das Internet sehr vielfältig ist kommt es ebenso mit vielen Gesetzten in Berührung. Wer in der Schweiz Informationen über Internet Gesetzte haben möchte, wendet sich am einfachsten an einen Anwalt.

#### 4.1.1. Onlinerecht

Hier eine Zusammenfassung von Rechtsfällen im Internet und deren Auswirkungen. Diese Fälle beziehen sich auf die Rechtslage in der Schweiz. Je nach Land weichen die Internet-Gesetzte ab.

##### 4.1.1.1. Datenmissbrauch

Fall: Herr Huber kontrolliert seine Kreditkartenabrechnung. Er findet auf dieser Abrechnung einen eigenartigen Betrag. In Mexico habe er eine Rolex-Uhr gekauft. Herr Huber war jedoch noch nie in Mexico. Ihm fällt ein, eine Buchung vor nicht all zu langer Zeit im Internet getätigt zu haben.

Urteil: Herr Huber ist höchstwahrscheinlich Opfer einer Social Engineering Attacke (Phishing). Nicht Herr Huber war in Mexico, dafür die Betrüger. Herr Hubers Kreditkartendaten wurden wahrscheinlich durch eine Phishing Website abgefischt. Herr Huber muss den Betrag bezahlen, da die Kreditkartenfirma mangelhafte Sorgfalt nachweisen kann.

##### 4.1.1.2. E-Banking

Fall: Herr Meier empfängt ein Email seiner Bank. Er wird darin aufgefordert auf einen Internet-Link zu klicken. Dort soll er sich authentifizieren um seine E-Banking Sicherheit zu erfahren. Nach Abschluss dieser Aktion durch Herr Meier erfährt er später, dass ein grosser Geldbetrag von seinem Konto an einen unbekanntem Empfänger überwiesen wurde.

Urteil: Auch hier handelt es sich um eine Social Engineering Attacke (Phishing). E-Banking-Systeme sind schwierig davor zu schützen. Wer jedoch die Sicherheitstipps der Bank befolgt, hat rechtliche gute Chancen. Herr Meier hat diese Tipps jedoch nicht befolgt und sein Geld verloren.

##### 4.1.1.3. Geldwäscherei

Fall: Herr Müller kann endlich seine Schulden loswerden. Er hat ein E-Mail erhalten, in welchem ihn ein Fremder um die Daten seines Bankkontos bittet. Dieser möchte über dieses Geldtransaktionen über das Konto durchführen. Einen Teil der übertragenen Summe könne Herr Müller für sich behalten. Die Transaktionen seien legal.

Urteil: Die E-Mail ist ein Hoax bzw. eine Lüge. Sobald Herr Meier die Daten des Bankkontos an den unbekanntem überweist ist er wieder Opfer eine Social Engineering Attacke (Phishing). Herr Müller hilft somit aber auch bei Geldwäscherei mit und macht sich strafbar. Auch in leichten Fällen kann dies zu Freiheitsstrafen von bis zu drei Jahren oder einer Busse führen.

#### 4.1.1.4. Jugendlicher Hacker

Fall: Das Ehepaar Meister hat einen minderjährigen Sohn. Dieser schreibt Viren und hackt im Internet. Vor nicht all zu langer Zeit ist er aufgefliegen. Er hat Firmen geschädigt, welche jetzt Schadensgeld fordern. Freunde der Eltern behaupten, sie müssen anstelle des Sohnes bezahlen.

Urteil: Im Grundsatz haftet der Sohn. Minderjährigkeit schützt vor Strafe nicht. Jedoch gibt es eine Ausnahme: Die Eltern müssen ihrer Aufsichtspflicht nachkommen, an sonst tragen sie Mitverantwortung. Die Eltern haben in diesem Fall jedoch nicht das technische Wissen.

#### 4.1.1.5. Tauschbörsen

Fall: Der 16 Jährige Lukas hat im Internet die Software eMule entdeckt. Mit dieser lassen sich Hollywood-Filme gratis herunterladen.

Urteil: Filme und Musik stehen unter Urheberrechtsschutz. Dennoch ist das kopieren in der Schweiz für den Privatgebrauch erlaubt. Verboten aber ist das anbieten dieser Filme. Die Tauschbörsen beinhalten ein grosses Risiko, da die Download-Programme während des Herunterladens den anderen Benutzern die Dateien bereits wieder bereitstellen.

#### 4.1.1.6. Texte kopieren

Fall: Frau Salisch kopiert einen Artikel einer Zeitschrift auf Ihre Website. Sie gibt die Quelle an. Einige Zeit später erhält sie ein Email der Zeitschrift-Redaktion mit der Bitte den Inhalt von Ihrer Website zu entfernen.

Urteil: Auch kopieren und veröffentlichter fremder Texte und Bilder stellt eine Urheberrechtsverletzung dar, unabhängig davon, ob eine Quelle genannt wird. Legal jedoch sind Zitate mit genauer Quellenangabe. Daher muss die genaue Textzeile angegeben werden. Eine weitere Möglichkeit wäre einen Internet-Link auf die Website mit dem Inhalt zu erstellen.

### 4.1.2. Grauzonen

Einige Schweizer Gesetze sind nicht fertig gestellt. Hier ein Auszug aus den „Grauzonen“ im Internet.

#### 4.1.2.1. E-Commerce Gesetz

Schutzmassnahmen für Online-Käufer sind noch nicht klar definiert. Die Schweizerische Stiftung für Konsumentenschutz hat eine parlamentarische Initiative gestartet.

Informationen: [www.konsumentenschutz.ch](http://www.konsumentenschutz.ch)

#### 4.1.2.2. Urheberrecht

Das Urheberrecht wird an das Internetzeitalter angepasst. Der Ständerat hat dies genehmigt. Vermutlich tritt das neue Gesetz 2008 in Kraft.

[www.urheberrecht.ch](http://www.urheberrecht.ch)

## 4.2. Illegalitätsbekämpfung

In der Schweiz gibt es inzwischen eine Zentrale Meldestelle für Internet-Kriminalität. Kobik leitet die Verdachtsfälle danach an die Kantone weiter, wo diese bearbeitet werden. Natürlich kann man sich auch direkt an die Polizei melden.

Laut dem Bundesamt für Polizei gehen mehrere Hundert Verdachtsmeldungen pro Monat bei der Meldestelle kobik.ch ein.

<http://www.kobik.ch/>

„Die nationale Koordinationsstelle zur Bekämpfung der Internet-Kriminalität (KOBIK) ist die zentrale Anlaufstelle für Personen, die verdächtige Internet-Inhalte melden möchten. Die Meldungen werden nach einer ersten Prüfung und Datensicherung den zuständigen Strafverfolgungsbehörden im In- und Ausland weitergeleitet.“

Zitat der Informationsseite <http://www.kobik.ch/> (Startseite, Zeile 2)

## 5. Interview mit Spezialisten

---

### 5.1. Schaffhauser Polizei, Beat Schaffitz

Auf Anfrage bei der Schaffhauser Polizei habe ich ein offiziell genehmigtes Interview mit Herr Beat Schaffitz vereinbaren können. Ich besuchte Herr Schaffitz auf dem Polizeiposten in Schaffhausen.

1. Was genau für eine Aufgabe haben Sie bei der Polizei?

Ich arbeite bei der Schaffhauser Kriminalpolizei. Hauptsächlich bearbeite ich Wirtschaftsdelikte. Unter anderem untersuchen wir PCs und Handys und werten die Daten darauf aus.

Generell verfolgen wir Verdachtsfälle, demnach surfen wir nicht den ganzen Tag im Internet und suchen nach Kriminellen, sondern reagieren auf Hinweise.

2. Gibt es viele Kriminalfälle im Internet?

Im 2007 untersuchten wir rund 50 Computer. Die meisten davon lieferten uns Beweismaterial. Hauptsächlich haben wir Fälle in den Bereichen Onlinebörsen und Pornografie.

3. Das Internet ist ein Netzwerk welches in der ganzen Welt verfügbar ist. Wie gehen Sie bei Rechtsfällen damit um? Wo stossen Sie an Grenzen?

Grundsätzlich ist der Tatort massgebend. Kriminaltaten von Minderjährigen werden mit einer Spezialregelung behandelt. Meistens also bearbeiten wir als lokale Polizei ein ausgeübtes Verbrechen an einem Computer in Schaffhausen, welches gemeldet wurde.

4. Zeigt Ihre Statistik eine Zunahme der Internet-Kriminalität?

Computertechnologien entwickeln sich rasend schnell. Immer mehr Personen verwenden das Internet. Die Kriminalität steigt mit der Grösse des Internets.

5. Sind Sie selbst schon Opfer von Malware (Schädling) geworden?

Ich hatte bereits Virenwarnungen auf meiner Anti-Virus Software, diese hat den Virus sofort erkannt und gelöscht. Generell verwende ich einen Firewall-Schutz und ein aktuelles Anti-Virus Programm um mich vor „Schädlingen“ zu schützen.

6. Wie reagieren Sie bei der Polizei auf die extrem schnelle Entwicklung im Internet?

Wir organisieren Workshops unter spezialisierten Polizisten, dort werden Informationen ausgetauscht.

## 5.2. Internetspezialist, David Wagner

Herr David Wagner arbeitet bei der Firma MTF Schaffhausen AG. Er ist Leiter der Hosting-Plattform. Er und sein Team verwalten verschiedenste Online-Dienste.

1. Ist die Internet-Kriminalität für Sie als Email und Web Provider in der Schweiz ein Thema?

Ja. Internetkriminalität spielt für uns eine grosse Rolle. Wir müssen unsere Infrastruktur und unsere Kunden vor kriminellen Taten schützen. Die Services, welche vom Internet erreichbar sind, müssen ausreichend geschützt und abgesichert werden. Gerade als E-Mail Provider ist es nicht immer einfach, Benutzerfreundlichkeit und Sicherheit zu kombinieren. Eine E-Mail Nachricht darf keinen SPAM und keine Viren enthalten. Jedoch sollte zum Beispiel eine eCard (elektronische Grusskarte) nicht als SPAM erkannt werden.

2. Sind Sie der Meinung, dass die Kriminalität im Internet zunimmt?

Das Internet ist ein stark wachsendes Medium, welches von immer mehr Personen genutzt wird. An Plätzen wo sich viele Menschen aufhalten, ist auch immer eine gewisse Kriminalität vorhanden. Besonders in einem so internationalen Platz wie dem Internet ist es schwierig alles zu kontrollieren und die Gesetze jedes Landes zu beachten. Was in der Schweiz illegal ist, kann in einem anderen Land über einen anderen Provider oder über einen anderen Server ohne Probleme und ohne Kontrolle durchgeführt werden.

Deshalb würde ich sagen, dass im Internet die Kriminalität nicht direkt zunimmt, es braucht jedoch immer bessere Schutzmassnahmen gegen Kriminelle.

3. Glauben Sie, dass das richtige Anwenden des Internets zum Eigenschutz beiträgt?

Auf jeden Fall. Denn ein grosser krimineller Akt muss über eine grosse Anzahl von vernetzten Rechnern geschehen. Da ein Angreifer nie die benötigten Rechner selber zur Verfügung stellen kann, werden die Rechner von Privatpersonen dazu benutzt um z.B. Angriffe auf einen Webserver durchzuführen. Dies geschieht über so genannte "Trojaner".

Jedoch kann nicht immer die Verantwortung auf den Anwender geschoben werden. Denn man muss ja auch kein Automechaniker sein, um ein Auto sicher fahren zu können. Hier sind auf jeden Fall die Softwarehersteller gefragt. Denn diese müssen die Software so programmieren, dass diese sicher ist und wenn dennoch ein Fehler auftaucht, muss dieser schnell behoben werden.

Die von einem Anwender eingesetzte Software darf nicht zu einem Sicherheitsrisiko werden, jedoch müssen sich auch die Anwender über die Risiken im Internet bewusst sein.

4. Würden Sie die Bevölkerung besser über Risiken im Internet Informieren?

Die grosse Aufgabe zur Absicherung des Internets liegt hier eher, wie gesagt, bei den Softwareherstellern als bei den Anwendern. Es müssen Grundlagen geschaffen werden, die das Internet sicherer machen. Als Privatanwender sollte man seinen persönlichen Fachhändler kontaktieren, damit dieser einem auf wichtige Punkte aufmerksam machen kann.

Informieren sollten sich jedoch vor allem Eltern, damit diese nachvollziehen können was Ihre Kinder im Internet machen.

5. Waren Sie selbst einmal Opfer der Kriminalität im Internet?

Als Provider ist man ständig Attacken aus dem Internet ausgesetzt, da kann ein Fehler oder ein Problem nicht ausgeschlossen werden. Jedoch wurde ich persönlich noch nie Opfer eines Virus oder einer Attacke.

6. Haben Sie einen Vorschlag um das Internet Sicherer zu machen?

Wie oben erwähnt, müssen die Grundlagen für ein sicheres Internet geschaffen werden. Diese müssen dann auch von den Providern genutzt werden. Denn es bringt nichts, wenn ein Mittel zur Verhinderung von zum Beispiel SPAM E-Mails vorhanden ist, jedoch niemand dieses einsetzt.

7. Wie viel Zeit verbringen Sie täglich im Internet?

Zu Zeiten von Breitband Internet und Flat-Rates kann man nicht mehr "im Internet" sein, sondern es ist Kommunikationsmedium welches man für das tägliche Leben benutzt. Während der Arbeit oder zu Hause rufe ich meine E-Mails ab, erhalte die neusten Sicherheitswarnungen per RSS-Feed, kommuniziere mit Partnern und Kunden, lese die neusten Nachrichten auf einer Website oder schaue nur kurz nach wie das Wetter morgen wird.

So gesehen bin ich täglich mindestens 6-10 Stunden "im Internet".

8. Haben Sie einen Sicherheits-Tipp für einen normalen Internet Benutzer?

Es gibt leider nicht 'diesen einen Tipp' sonder es gibt viele Punkte zu beachten. Jedoch wenn möglich einen getrennten Rechner für das normale Surfen, wo die ganze Familie zugriff hat, benutzen und einen separaten Rechner für Bank- und Geschäftstätigkeiten. Ein Privatanwender sollte sich beim Fachhändler beraten lassen, welche Software für die benötigte Tätigkeit geeignet ist und was bei dieser beachtet werden muss.

## 6. Schlusswort

---

Das Arbeiten am Thema Internet-Kriminalität hat mir Spass gemacht. Ich hatte vor allem anfangs Schwierigkeiten mit der Volumenbegrenzung der Arbeit. Nach mehrfachem überarbeiten konnte ich dem Umfang reduzieren. Leider musste ich somit auch mein Ziel etwas verändern. Zu Beginn wollte ich die Arbeit für Laien wie auch professionelle IT Anwender interessant gestalten. Aufgrund der Verkleinerung welche ich vornehmen musste, fehlen interessante Details für Computer Profis. Ich bin der Meinung, dass diese Arbeit dennoch für Internet Anwender wichtig ist, denn Sie informiert umfassend über Gefahren im Internet.

Ich hatte bereits viel Vorkenntnis bevor ich die Arbeit begann, aufgrund meiner beruflichen Tätigkeit. Mein Vorgehen bestand darin, dass ich mich vor dem Schreiben über verschiedenste Themen informierte. Anschliessend versuchte ich die Arbeit gut zu strukturieren. Dies war leider nicht ganz einfach, da einige Themen ineinander verfliessen. Schlussendlich konnte ich aber eine saubere Struktur erstellen. Gleich darauf begann ich mit schreiben. Leider wurde die Arbeit wie erwähnt etwas zu umfangreich. Ich kürzte verschiedenste technische Bereiche heraus und gestaltete die Arbeit somit verständlicher für einen Laien.

## 7. Quellen

---

Folgende Quellen wurden verwendet:

### 7.1. Formen der Internet-Kriminalität

<http://www.ejpd.admin.ch/>

<http://de.wikipedia.org/>

### 7.2. Sicherer Umgang mit dem Internet

<http://www.webreference.com/>

<http://www.watchguard.com/>

<http://de.wikipedia.org/>

### 7.3. Gesetze in der Schweiz

Texte von PCTipp Artikel Internet Recht vom April 2007 abgeleitet.

<http://www.pctipp.ch/data/filesserver/heftarchiv/2000/07/0728ille.pdf>

## 8. Kontakt

---

Ich freue mich über Ihr Feedback. Gerne beantworte ich Ihre Kritik, Frage, Anregung oder Idee per Email.

Florian Meier  
Schaffhausen  
Schweiz (CH)

Email: [florian.meier@mtf.ch](mailto:florian.meier@mtf.ch)