

**Zeitschrift:** Comtec : Informations- und Telekommunikationstechnologie = information and telecommunication technology  
**Herausgeber:** Swisscom  
**Band:** 81 (2003)  
**Heft:** 10

**Artikel:** Wer wird das bezahlen?  
**Autor:** [s. n.]  
**DOI:** <https://doi.org/10.5169/seals-876693>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 17.03.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

# Wer wird das bezahlen?

Im November letzten Jahres wurde Lisa Chen in einem spektakulären Prozess in den USA zu neun Jahren Haft und einer Schadensersatzzahlung von 11 Mio. US-\$ verurteilt. Was hatte sich die Frau zu Schulden kommen lassen?

Das Gericht befand sie für schuldig, etwa 600 000 Raubkopien von «Norton AntiVirus», «Norton SystemWorks», «Norton Personal Firewall» und «pcAnywhere» in Umlauf gebracht zu haben. Mit Lisa Chen wurde nur einer von vielen tausend professionellen Raubkopierern zur Rechenschaft gezogen.

## Software-Piraterie nimmt drastisch zu

Lisa Chen büsst ihre Strafe für ein Delikt ab, das nicht nur bei privaten PC-Anwendern verbreitet ist, sondern auch bei Unternehmen als Praxis um sich greift. Da gibt es die Firmen, die sich des Problems noch nicht ausreichend bewusst sind und unwissentlich raubkopierte Produkte im Einsatz haben. Und dann gibt es noch jene Unternehmen, die gerade in wirtschaftlich schwierigen Zeiten im Einsatz von Raubkopien eine willkommene Sparmassnahme sehen. In einer Untersuchung zur Raubkopierate hat die

Business Software Alliance (BSA, Homepage: [www.bsa.de](http://www.bsa.de)) im zweiten Jahr in Folge einen weltweiten Anstieg festgestellt. 40% aller eingesetzten Software ist demnach illegal erworben oder raubkopiert. Der geschätzte Schaden im Jahr 2001 betrug weltweit umgerechnet 12,26 Mia. €.

## Spamming als Verbreitungsweg

Die Zahlen machen deutlich, dass sich Softwarepiraterie längst zu einer florierenden kriminellen Branche entwickelt hat. Der Handel mit raubkopierter Software findet häufig via E-Mail-Spamming statt. Mit Spamming (von «spill» = überlaufen und «cram» = vollstopfen) ist das unaufgeforderte Zusenden von E-Mails gemeint. Meistens ist die E-Mail-Flut lästig, aber nicht immer steckt eine kriminelle Absicht dahinter. Wie erkennt man jedoch, ob es sich um einen harmlosen Werbefriede oder um ein Angebot von raubkopierter Software handelt? Unter [www.symantec.de/region/de/spam-](http://www.symantec.de/region/de/spam-watch.html)

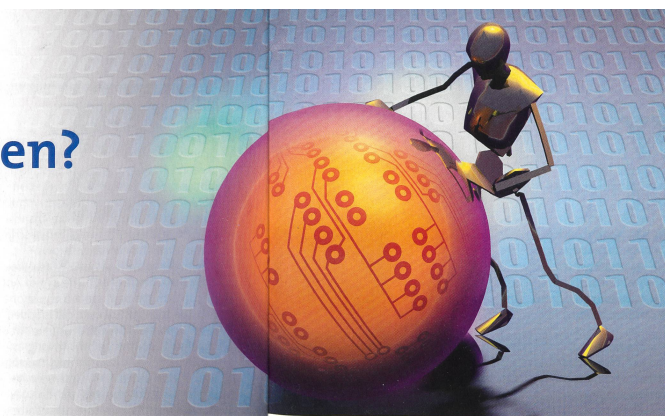
[watch.html](http://www.symantec.de/region/de/spam-watch.html) finden sich Warnhinweise für den richtigen Umgang mit Spam-Mails und Tipps, wie man auf verdächtige Software-Angebote reagieren sollte.

## Gefahren für Nutzer

Bei Raubkopien gilt: Die Lust am Sparen kann einen ganz schön teuer zu stehen kommen. Wer Raubkopien kauft und einsetzt, läuft Gefahr, sich Viren auf seinem Rechner oder System einzufangen. Wer weiss schon, ob er mit der Raubkopie eine Software installiert, die sensible Daten auf dem Rechner ausspioniert? Die Software kann darüber hinaus Fehler, so genannte «Bugs», enthalten, die das Betriebssystem des Rechners schädigen können. Bei gefälschter Software erhält man ein Produkt, das nicht annähernd so leistungsfähig ist, wie die Originale. Zudem sind viele dieser Angebote via Spam-Mail einfach eine Masche, um an Kreditkartennummern heranzukommen. Vertrauensselige Kunden erhalten überhaupt kein Produkt, dafür wird Geld von ihrer Karte abgebucht.

## Wer zahlt den Schaden?

Viele private PC-Benutzer, aber auch manche Verantwortliche in Unternehmen wollen nicht wahrhaben, dass Software-Piraterie kein Kavaliärsdelikt ist. «Die meisten unserer Geschäftskunden gehen sehr verantwortungsbewusst mit ihren Nutzungsrechten an unserer Software um», erläutert Michael Hoos, technischer Leiter bei Symantec. «Letztlich ist der ehrlich zahlende Kunde das Opfer



Mit einer Raubkopie kann eine Software installiert werden, die sensible Daten auf dem Rechner ausspioniert.

einer Straftat, die andere immer noch verharmlösen», so Michael Hoos weiter. Die Schäden gehen weit über die finanziellen Einbußen hinaus, die der betroffene Software-Hersteller verkraften muss: Raubkopien von Software treiben die Preise nach oben. Je mehr Umsatzeinbußen ein Unternehmen durch gestohlene Software erleidet, umso weniger kann in die Entwicklung neuer Produkte und Innovationen investiert werden. Aber damit nicht genug: Jeder Umsatzausfall für einen Software-Hersteller bedeutet weniger Umsatz für Zuliefererfirmen, für Hersteller von Verpackung, Datenträgern und Handbüchern, für den Fachhandel und Serviceanbieter.

Jeder Arbeitsplatz bei einem Software-Hersteller, so rechnet die BSA vor, bedeutet weitere 6,7 Arbeitsplätze in verbundenen Branchen. «Der Schaden, den Software-Räuber Software-Unternehmen zufügen, kostet Arbeitsplätze, ist innovationsfeindlich, hemmt das Wirtschaftswachstum und schadet letztlich uns allen», resümiert Michael Hoos. □

Symantec (Switzerland) AG  
Grindelstrasse 6  
CH-8303 Bassersdorf  
Tel. 01 838 49 32  
Fax 01 838 49 01  
E-Mail: [Heike\\_Faller@symantec.com](mailto:Heike_Faller@symantec.com)

## Summary

### Who will pay for it?

Software piracy has long been a thriving field of crime. Trading with pirated software often takes the form of e-mail spamming, or the sending of unsolicited e-mails. An investigation of the piracy rate by the Business Software Alliance has revealed a worldwide increase for the second year running. According to the study, 40% of all software used has been illegally obtained or pirated. Estimated worldwide damages for the year 2001 amounted to around 12.26 billion dollars. Is the money saved through piracy really a saving? Sometimes it can end up being far more expensive than buying the original software.

## Typischer Hacker ist unter 21 Jahre alt

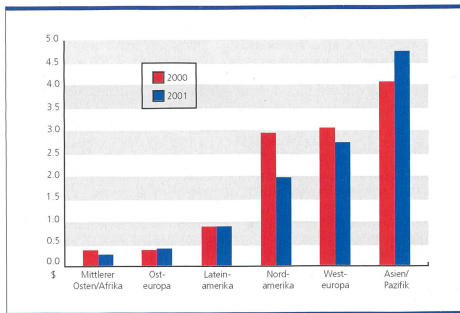
Der typische Internet-Hacker ist männlich, zwischen 16 und 21 Jahren alt und lebt noch bei seinen Eltern. Zu diesem Ergebnis kommt das deutsche Kriminalistische Institut des Bundeskriminalamts (BKA) ([www.bka.de](http://www.bka.de)) in einer Studie über «Account-Missbrauch im Internet». Das BKA hat gemeinsam mit der Universität Münster einen Fragebogen entwickelt, der an beteiligte Staatsanwaltschaften, Gerichte und Eltern von Tatverdächtigen verschickt wurde. 599 Fragebögen wurden ausgewertet. Drei Typen von Hackern konnten ausgemacht werden.

Der Studie zufolge gibt es einen «typischen» Hacker, 65,8% (373 Mitglieder) der Täter zählen zu dieser Gruppe. Er ist männlichen Geschlechts, zwischen 16 und 21 Jahren alt und lebt bei seinen Eltern. Er hat eine mittlere oder gehobene Schulbildung und mittlere bis hohe Computerkenntnisse, die er sich autodidaktisch erworben hat. Gründe für den Account-Missbrauch sind in dieser Gruppe in erster Linie wirtschaftlicher Natur oder um auszuprobieren, was geht. Der durchschnittliche Schaden, den diese Gruppe anrichtet, beträgt 388 Euro.

Die zweitgrösste Gruppe der «untypischen Täter» (119 Mitglieder) ist auch männlich, aber älter als die typischen Täter und lässt sich wegen vielfältiger Möglichkeiten zur Lebensgestaltung nicht eindeutig kategorisieren. Die untypischen Täter haben mehr Geld und mehr PC-Erfahrung als die erste Gruppe. Der Schaden, den sie angerichtet haben, ist mit durchschnittlich 429 Euro nur geringfügig grösser als jener der typischen Täter.

Die dritte und kleinste Gruppe besteht aus Frauen (5,8%, 35 Mitglieder). Im Schnitt sind sie 34,7 Jahre alt und haben geringere EDV-Kenntnisse und langsamere Rechner als die männlichen Täter. Ihr Hauptmotiv besteht meistens auch im Ausprobieren oder in wirtschaftlichen Erwägungen. Nur 5% von ihnen wussten, dass sie eine strafbare Handlung begehen. Im Mittel waren die Täter 23 Jahre alt, insgesamt 72,2% von ihnen lebten während der Tatbegehung bei ihren Eltern. Das Hauptmotiv bei allen drei Gruppen sind wirtschaftliche Gründe (51,3%), zweit-häufigstes Motiv ist das Ausprobieren (33,1%).

Info: Homepage: [www.bka.de/informationen/account\\_missbrauch.pdf](http://www.bka.de/informationen/account_missbrauch.pdf)  
Quelle: pte-online



Verluste nach Regionen in Milliarden US-\$.