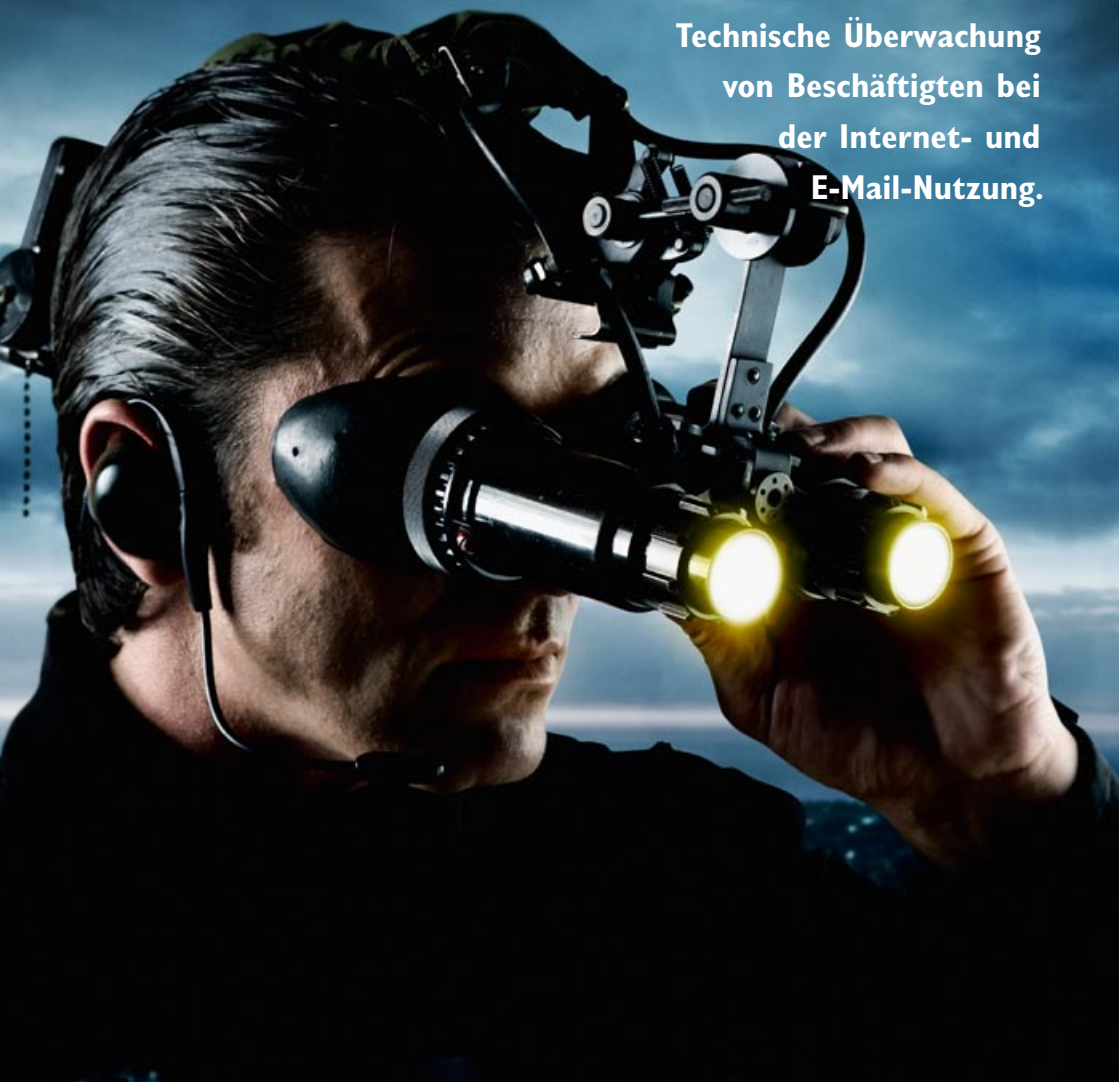


# RÄCHER

## DER ENTERBTEN DATEN

Technische Überwachung  
von Beschäftigten bei  
der Internet- und  
E-Mail-Nutzung.



**GPA**

GEWERKSCHAFT DER PRIVATANGESTELLTEN



## Was ist die IG work@IT?

work@IT ist die Interessengemeinschaft der GPA für Menschen in der Informations- und Kommunikationstechnologie. Wir sind eine basisdemokratische, gewerkschaftliche Plattform von IT-Spezialist/-/innen, unabhängig davon in welcher Branche wir arbeiten.

Von Angestellten über Freie Dienstverträge und Werkverträge bis zu Gewerbeschein, repräsentieren wir in unseren Beschäftigungen die Mannigfaltigkeit der „New Economy“.

### Wer sind wir?

Wir sind Programmierer/-/innen, Netzwerkadministrator/-innen, Systemadministrator/-innen, Techniker/-innen, Content Providers, Entwickler/-innen, Künstler/-innen, Medienspezialist/-innen, Web Designers, Web Masters & Mistresses, Soft Ware Testers, Projektmanager/-innen, Telekommunikationsspezialist/-innen, Medienbeobachter/-innen, Datenschützer/-innen und viele mehr...

### ... kurz wir sind IT-Spezialist/-innen!

Unsere Ziel ist Erfahrungsaustausch, Kommunikation und Vernetzung mit anderen IT-Beschäftigten.

Wir unterstützen Dich in der Artikulation und bei der Durchsetzung Deiner Anliegen, Wünsche und Forderungen im Arbeitsleben, auf politischer Ebene und in den Medien.

Auch wenn Du kein Gewerkschaftsmitglied bist, kannst Du Dich kostenlos in unsere IG eintragen und auf diese Weise unser Service besser kennen lernen.

work@IT steht Dir als persönlicher Frame mit individueller Beratung und Vertretung zur Seite:

## JOIN US!



## Vorwort

Die intensive Beschäftigung mit technologischen Veränderungen am Arbeitsplatz und ihre Auswirkungen auf die Arbeitnehmer/-innen haben in der GPA eine lange Tradition. Im Bereich der Kommunikationstechnologien kann man in den letzten Jahren in der Tat von revolutionären Veränderungen sprechen, welche für die Beschäftigten auch Risiken und Gefahren beinhalten.

Eine dieser Gefahren ist die Möglichkeit der technischen Überwachung bei der Internet und E-Mail-Nutzung durch Arbeitgeber. Für den Großteil der von der GPA vertretenen Arbeitnehmer/-innen gehört die Nutzung von elektronischen Netzwerken zur alltäglichen Arbeit. Für die Gewerkschaft und die Betriebsrät/-innen wirft dieses Faktum eine Reihe von technischen und rechtlichen Fragen auf, welche in der „traditionellen“ Arbeitswelt nicht bekannt waren. Ich denke, dass es mit dieser Broschüre der GPA-Interessengemeinschaft work@IT gelungen ist, sowohl einen guten Überblick über aktuelle technische Entwicklungen, als auch nützliche Tipps für betroffenen Arbeitnehmer/-innen und Betriebsrät/-innen zu geben.

Diese Broschüre ist auch ein Ausdruck davon, dass von der Arbeit der GPA-Interessengemeinschaften, einem noch relativ jungen Strukturelement unserer Gewerkschaft, zukunftsweisende Impulse für die gesamte Arbeitswelt ausgehen.

**Wolfgang Katzian**

GPA-Vorsitzender

**“Paranoia heißt, alle  
Fakten zu kennen”**

(William S. Burroughs)



# Einleitung

Durch die neuen Informations- und Kommunikationstechnologien wandelt sich unsere Kommunikation am Arbeitsplatz. Heute ist theoretisch jeder Schritt eines/r Beschäftigten am PC zu überwachen.

In der betrieblichen Praxis der Unternehmen wird die Nutzung von Inter- und Intranet sehr unterschiedlich gehandhabt. Einige verfügen über keinerlei Regelungen, andere verhängen Verbote oder kontrollieren durch spezielle Software das Online-Verhalten der Beschäftigten. Immer öfter teilen uns Arbeitnehmer/-innen mit, dass sie in ihrer Firma gefragt wurden, warum sie die Telefonnummer der GPA gewählt hätten.

## **Woher weiß die Firma welche Telefonnummern von den Beschäftigten angewählt wurden?**

Systemadministrator/-innen wenden sich an die Interessengemeinschaft work@IT, da ihr/e Chef/-in ihnen den Auftrag gegeben hat die E-Mails von Beschäftigten an sein/ihr E-Mail-Account weiterzuleiten ohne, dass die Beschäftigten etwas davon bemerken dürfen.

Um es vorweg zu nehmen: Als Mitarbeiter/-in in einem restriktiv aufgebauten Unternehmensnetzwerk hat man mit technischen Mitteln praktisch keine Möglichkeiten, sich vor allzu neugierigen Vorgesetzten zu schützen. Nur eine bewusste, verantwortungsvolle Nutzung der Technologie und organisatorische Regelungen (Betriebsvereinbarungen) durch die betriebliche Interessenvertretung (Betriebsrat) können der totalen Überwachung einen Riegel vorschieben oder sie zumindest in die Illegalität drängen.

Eine gesunde Paranoia kann also bei der Nutzung aus Firmennetzwerken nicht schaden.

Darum hat die Interessengemeinschaft work@IT die Initiative „Rächer der enterbten Daten“ ins Leben gerufen. Diese Kampagne soll helfen, Sie für grundsätzliche Möglichkeiten der Arbeitsplatzüberwachung und Wege zur Vorbeugung zu informieren.

## ein tipp

Auch wenn Sie keine der von uns beschriebenen Anzeichen für eine Überwachung an ihrem Arbeitsplatz finden, kann es dennoch möglich sein, dass Sie von Ihre(m)-r Chef/-in kontrolliert werden. Daher sollten Sie das Thema Arbeitsplatzüberwachung offen gegenüber Ihrem Betriebsrat ansprechen oder sich an die IG work@IT wenden:

<http://www.interesse.at/it>

# Inhaltsverzeichnis

|  |           |
|--|-----------|
| <b>1. Warum Firmen die Online-Aktivitäten von Beschäftigten überwachen? .....</b>          | <b>8</b>  |
| <b>2. Zahlen, Daten, Fakten zu Überwachung und Surfverhalten ...</b>                       | <b>8</b>  |
| <b>3. Der böse Systemadministrator? – Ein ungerechtes Urteil. ....</b>                     | <b>10</b> |
| <b>4. Hat Ihr Chef Ihnen schon zur neuen Freundin gratuliert? Ihre Outlookdaten.....</b>   | <b>11</b> |
| <b>5. Spielt Ihr Boss „Stille Post“? Ihre E-Mails .....</b>                                | <b>11</b> |
| <b>6. Wie privat sind private Dateien? .....</b>   | <b>12</b> |
| <b>7. Deus ex machina? – Techn. Grundlagen v. Firmennetzwerken</b>                         | <b>12</b> |
| <b>8. Die Überwachung am PC .....</b>  | <b>13</b> |
| <b>9. Cookies &amp; Caches – Spuren beim Browsen.....</b>                                  | <b>13</b> |
| 9.1. Hast Du einen Keks? Was sind Cookies? .....   | 13        |
| 9.2. Löschen von Cookies .....   | 15        |
| 9.3. Anlegen von Cookies verbieten .....   | 15        |
| 9.4. Wie man Cookies findet, wie man sie sich ansehen kann und wie man sie verbietet ..... | 16        |
| 9.5. Akzeptanz von Cookies .....   | 17        |
| 9.6. Ansehen der vorhandenen Cookies.....  | 17        |
| <b>10. Cache free – Der „Verlauf“ der „Historie“ .....</b>                                 | <b>18</b> |
| 10.1. Ansehen des Caches .....   | 18        |
| 10.2. Den Cache finden, ansehen und löschen .....  | 19        |
| 10.3. Beeinflussen Sie den Verlauf der Geschichte – Ihre History ...                       | 19        |
| 10.4. Die Verlaufsliste finden, anzeigen, löschen .....                                    | 19        |
| <b>11. Spionageprogramme .....</b>   | <b>21</b> |
| 11.2. Tastensammler .....  | 23        |
| 11.3. Produktinformation zu Spionagesoftware .....   | 25        |
| 11.4. Was kann ich tun? .....  | 29        |

|  |           |
|--|-----------|
| <b>12. Die zentrale Überwachung – Firewalls, Router, Proxy</b> | <b>32</b> |
| 12.1. Firewalls  | 32        |
| 12.2. Router   | 32        |
| 12.3. Proxy-Server   | 32        |
| 12.4. Die Probleme   | 34        |
| <br>   |           |
| <b>13. Servus Server! – Software für den Diener</b>            | <b>35</b> |
| 13.1. Produktinformation                                       | 36        |
| 13.2. .. und wie man sich dagegen wehrt                        | 40        |
| <b>14. Spionage-Hardware</b>                                   | <b>41</b> |
| <b>15. Wie gut ist Ihr Passwort?</b>                           | <b>42</b> |
| 15.1. Passwortqualität   | 42        |
| 15.2. Testen Sie Ihr Passwort                                  | 43        |
| 15.3. Wie macht man gute Passwörter                            | 43        |
| 15.4. Passwortschutz von Word-Dateien                          | 44        |
| <b>16. Verschlüsse Dich</b>                                    | <b>44</b> |
| 16.1. Der einfachste Weg: E-Mail-Verschlüsselung               | 44        |
| 16.2. Tierliebe: work@IT liebt aber Gnu                        | 47        |
| 16.3. So oft wie möglich verschlüsselte Seiten verwenden       | 48        |
| 16.4. Dienste maskieren und Ziele verbergen                    | 49        |
| <b>17. Mission accomplished</b>                                | <b>52</b> |



# I. Warum Firmen die Online-Aktivitäten von Beschäftigten überwachen?

- Das Aufdecken von verschwendeten Zeitressourcen durch privates Surfen, E-Mails oder Spielen am PC.
- Der Schutz der unternehmensinternen Netzinfrastruktur, die durch „Napstern“ (das Tauschen von Musik, Videos im Internet) oft an Kapazitätsgrenzen stößt.
- Die Aufdeckung von kriminellen Machenschaften am Arbeitsplatz. Firmen befürchten einen Imageschaden, wenn Angestellte rechtsradikale oder pornographische Inhalte in Umlauf bringen.
- Der Schutz von Betriebsgeheimnissen
- Aber es geht auch darum einfach, gezielte Informationen über unliebsame Mitarbeiter/-innen zu sammeln, die eine fristlose Entlassung oder Maßregelungen oft erst möglich machen.

## 2. Zahlen, Daten, Fakten zu Überwachung und Surfverhalten

Diese Befürchtungen und Gründe für Überwachungsmaßnahmen werden auch mit Zahlen untermauert:

So behauptet eine Studie von Focus online (<http://www.focus.de>), **dass 75% aller Zugriffe auf Sex-sites zwischen 9:00 und 17:00 stattfinden.**

Eine Befragung durch IDC (<http://www.idc.com>) will herausgefunden haben, dass **30-40% der Netzwerkbelastung durch nicht arbeitsrelevante Aktivitäten** verursacht wird.

Eine Befragung von 1000 Unternehmen durch das Softwarehaus „Sterling Commerce“ (<http://www.wirtschaftsblatt.at> am 9.9.2000) behauptet, dass das **private Surfverhalten ihrer Angestellten das Ausmaß von 17 Arbeitstagen oder rund 53 Milliarden Euro jährlich** ergäbe.

Diese Ängste von Unternehmern sind mit ein wenig gutem Willen und Einfühlung in die Interessenlage von Firmen zumindest nachvollziehbar, ihre Konsequenzen in vielen Situationen aber keinesfalls tolerierbar.

Aufklärung der Beschäftigten über technische Überwachungsmöglichkeiten ist gefragt. Denn die Überwachung ist bereits im Gange. So wurden im Jahr 2000

in den USA bereits 38% der versandten Emails mitgelesen (<http://www.chip.de> am 31.12.2000).

Das Beratungsunternehmen „American Management Association“ gibt für 2001 an, dass 63% aller Bildschirmarbeitsplätze überwacht werden (<http://www.handelsblatt.com> am 16.7.2001).

---

**Der Big Brother Award**  
**(<http://www.bigbrotherawards.at>) schätzt**  
**die Quote der überwachten Bildschirm-**  
**arbeitsplätze in den USA sogar auf etwa 80%.**

---

Doch nicht erst der eigentliche Einsatz, sondern schon alleine die Ankündigung der unternehmensweiten Installation von Überwachungsprogrammen verändert das Surfverhalten der Angestellten dramatisch: Nach Aussagen von Carsten Rau, Geschäftsführer der Protectcom (<http://www.protectcom.de>), wird die Onlinezeit nach Ankündigung der Installation um bis zu 90% produktiver genutzt.

Aber auch für Maßregelungen und arbeitsrechtliche Konsequenzen auf Grund von Überwachungsprotokollen sind inzwischen einige Beispiele bekannt – wenn auch überwiegend aus den USA. So wurden beispielsweise im Jahre 1999 23 Angestellte der New York Times wegen des Versands angeblich obszöner Mails entlassen und die Firma Dow Chemical hat im Jahr 2000 24 Angestellte gekündigt und weitere 235 abgemahnt, weil sie „schmutzige Mails“ geschrieben hätten. Auch die bayrische Staatskanzlei hat aufgrund von Überwachungsprotokollen bereits 12 Beamte abgemahnt.





### 3. Der böse Systemadministrator? Ein ungerechtes Urteil

Der/Die Systemadministrator/-in hat Zugriffsrechte auf alle Rechner im Unternehmen. Er/Sie kann somit auch Ihre persönlichen Daten einsehen. Der/Die Administrator/-in hat die Möglichkeit, auf jedem einzelnen Rechner z.B. Software zu installieren oder Virenskans durchzuführen und kann somit nicht nur auf Ihre privaten E-Mails, sondern auch auf Ihren Terminkalender, Ihre gespeicherten Adressen und auf private Dateien zugreifen.

**Systemadministrator/-innen sind die personellen Schlüsselstellen der firmeninternen Netzwerke.**

Sie wissen durch ihre Erfahrung am besten welche technischen Möglichkeiten zur Überwachung bestehen und sind deshalb besonders sensibel im Umgang mit der Privatsphäre der Beschäftigten. Leider sind sie in der unangenehmen Lage Weisungen der Geschäftsführung zur Überwachung durchzuführen. Die Interessengemeinschaft work@IT legt deshalb großen Wert darauf, dass nicht die Sysadmins zu Sündenböcken der Überwachung gestempelt werden. Die Auftraggeber der Auswertungen in den Unternehmen sind das Problem!

## 4. Hat Ihr Chef Ihnen schon zur neuen Freundin gratuliert? >> Ihre Outlookdaten

Der/Die Systemadministrator/-in ist in der Lage alle Termine, Adressen und Aufgaben, die sie in Ihrem Terminkalender oder Organizer (z.B. Outlook) gespeichert haben, einzusehen.

Er/Sie hat sogar die Möglichkeit, diese zu verändern, ohne dass Sie es merken. Selbst wenn Sie die Termine oder Notizen als „privat“ kennzeichnen, hindert das den/die Administrator/-in keineswegs Einblick zu nehmen.

## 5. Spielt Ihr Boss „Stille Post“? Ihre E-Mails

In vielen Unternehmen werden die versandten E-Mails der Beschäftigten mitgelesen oder überprüft. Die Unternehmen begründen diese Tatsache obszöne, pornographische oder verfassungsfeindliche Inhalte unterbinden zu wollen.

Die private E-Mail-Korrespondenz von Arbeitnehmer/-innen unterliegt ebenso der gesetzlich geschützten Privatsphäre wie private Telefonate oder Briefe.

### **Dabei gibt es mehrere Möglichkeiten:**

So wie beim Zugriff auf Ihre „Outlook-Termine“ und Notizen kann der/die Administrator/-in natürlich Ihren „Posteingang“ ansehen – aber auch die „gelöschten Objekte“. Wesentlich effizienter für Systemadministratoren/-innen ist der Einsatz von speziellen Programmen, die den gesamten E-Mailverkehr eines Unternehmens überwachen und auswerten können. So ist es möglich jedes Ihrer E-Mails nach bestimmten Schlagworten, Dateien oder Empfängern auszuwerten – und Ihre/-m Administrator/-in oder Vorgesetzte/-n „serviceorientiert“ davon automatisch in Kenntnis zu setzen.

Selbst Bilder oder Dateianhänge können schon analysiert werden. Wenn sehr viel „hautähnliche Farbe“ im Bild vorkommt, schlagen die meisten Programme Alarm.

## 6. Wie privat sind private Dateien?

Da der/die Systemadministrator/-in Einblick auf das gesamte System Ihres Computers am Arbeitsplatz hat, sogar eingelegte CD-ROMs, Disketten oder auch auf Ihre lokale Festplatte, kann er natürlich sämtliche Dateien, die Sie auf Ihrer Festplatte oder im unternehmensinternen Netzwerk ablegen, öffnen, ändern oder löschen.

Hier haben Sie kaum Möglichkeiten zu überprüfen, ob es Eingriffe in Ihre persönlichen Daten gibt. Viele Programme, beispielsweise auch Microsoft Office, Adobe Acrobat (PDF-Dateien), WinZip etc. lassen es daher zu, wichtige Dokumente durch ein Passwort zu schützen. Achtung! Nicht jeder Passwortschutz ist sicher. Microsoft-Office-Programme sind seit der Version 97 relativ sicher (mit Ausnahme von Access) aber besonders ältere Programmversionen oder nicht so weit verbreitete Programme zeigen oftmals große Mängel im Passwortschutz und können daher umgangen werden, wenn man es darauf anlegt. Doch besser ein schlechter Passwortschutz als gar keiner, denn so können Sie die Einsicht Fremder in die Dateien zumindest erschweren. Vor dem Löschen können Sie Ihre Dateien jedoch nicht bewahren.

## 7. Deus ex machina? – Technische Grundlagen von Firmennetzwerken

Um zu veranschaulichen, an welchen Punkten sich Zugriffsmöglichkeiten für die Neugierde Ihres Chefs ergeben, wollen wir eingangs die prinzipiellen technischen Grundlagen der Kommunikation von einem Firmennetzwerk in das Internet darstellen.

Jede Kommunikation aus einem Firmennetzwerk mit dem Internet, egal ob Email, dass WorldWideWeb oder andere Services wie Telnet oder FTP, geschieht über eine zentrale Stelle – das sogenannte „Gateway“ – das Portal ins weltumspannende Netz.

Dieses Gateway, das es in unterschiedlichen Ausformungen wie zum Beispiel „Router“, „Firewall“ oder „Proxy-Server“ gibt, stellt die Verbindung zwischen den Netzen her. Diese „Einfahrt“ muss jede Information passieren.

Hier ergeben sich schon zwei Schnüffelpunkte: Die einzelnen PCs im Unternehmen – eher für dilettantische und leicht erkennbare Attacken geeignet – und der zentrale Übergangspunkt zwischen den Netzen, wo man schon viel eleganter und sicherer lauschen kann.

---

**Als Erstes wollen wir uns der Überwachung am PC widmen. Zur zentralen Überwachung kommen wir später.**

---

## 8. Die Überwachung am PC

Viele Anwendungen und Betriebssysteme bieten selbst genügend Funktionen, die es Neugierigen möglich machen, eine Menge über die Surf- und E-Mail-Gewohnheiten eines Users in Erfahrung zu bringen. Doch die Auswertung dieser Informationen ist mühsam und zeitaufwändig und eignet sich nur zur Kontrolle einzelner unliebsamer Mitarbeiter/-innen, aber nicht zur unternehmensweiten Überwachung. In vielen Fällen protokollieren Anwendungen die Aktivitäten des Users, um die Betriebs-Stabilität zu gewährleisten (Log-Protokolle), um Ressourcen durch das Zwischenspeichern von aus dem Internet abgerufenen Inhalten zu schonen (Cache) oder auch, um den Komfort des/der Benutzer(s)/-in zu erhöhen und die Arbeit am PC angenehmer zu machen (Cookies). Für alle gilt, dass diese Anwendungen die Informationen in Form von Dateien auf der lokalen Festplatte oder auf zentralen Firmen-Servern ablegen.

---

**Alles was in einem Netzwerk erst einmal als Datei existiert, ist durch System-administrator/-innen und Vorgesetzte einsehbar!**

---

## 9. Cookies & Caches – Spuren beim Browsen

Spuren beim Surfen hinterlässt man an vielen Stellen. Vom Server der Zielseite, über den Proxy von Firmen oder Internet-Providern, auf Netzwerkwegen, die ausgewertet werden können bis zu zahlreichen Spuren, die am lokalen PC hinterlassen werden.

### 9.1. Hast Du einen Keks? Was sind Cookies?

“Cookies“ wurden von der Firma Netscape – einst der Internet-Browser-Hersteller mit dem größten Marktanteil – entwickelt. Cookies sind bislang die einzige direkte Möglichkeit, Informationen aus dem Internet auf dem lokalen PC abzulegen. Durch diese technische Neuerung, nämlich die Möglichkeit des Speicherns von Daten auf der Festplatte des Benutzers, wurde immer wieder die Gefahr des Auslesens und Löschens von persönlichen Daten über das Internet prophezeit. Eine Befürchtung,

die sich nicht bestätigt hat, da durch die reine Verwendung von Cookies es noch niemandem gelungen ist, geheime Daten zu löschen oder auszuspionieren.

Der Zweck der Erfindung war durchaus ein nobler: Durch das Speichern von Informationen auf dem lokalen PC war es möglich, dass eine Internet-Seite eine/-n Benutzer/-in – oder zumindest dessen/deren PC – „wiedererkennt“, was bis dahin nicht möglich war.

Cookies sind also Daten, die von Websites automatisch auf Ihrem Rechner gespeichert werden. Dadurch erkennt eine Internetseite Sie bei wiederholtem Zugriff wieder. Außerdem sind Cookies bei den meisten Shopsystemen aber auch vielen anderen Anwendungen im Internet aus technischen Gründen unbedingt notwendig. Viele Shops im Internet funktionieren überhaupt nur durch diese Cookies.

Leider missbrauchen insbesondere Unternehmen aus der Branche der Internet-Werbung diese Cookies derart, dass sie unbedachte User bei ihrem Surfverhalten beobachten können.

Cookies verraten auch sehr viel über Ihre Internet-Gewohnheiten und ein flüchtiger Blick auf die Festplatte kann viel über das Surfverhalten ihre(s)/-r Besitzer(s)/-in aussagen. Beispielsweise schreibt der Internet-Explorer von Microsoft diese Cookies in Form von kleinen Dateien, die schon durch ihren Namen die Gewohnheiten des Users ausdrücken können:

|                                     |                      |
|-------------------------------------|----------------------|
| karl.pick@ebay.com.txt              | geändert am 24.12.04 |
| karl.pick@support.microsoft.com.txt | geändert am 24.12.04 |
| karl.pick@amazon.de.txt             | geändert am 24.12.04 |

---

### **Ein Leichtes zu erraten, was an diesem Tag so alles getan wurde...**

---

Wenn man diese Dateien öffnet – das geht einfach mit einem Texteditor oder einem Schreibprogramm – offenbaren Sie noch mehr Details, etwa welche Kategorie von Bildern Sie bevorzugen oder wie oft Sie Suchanfragen in einer Suchmaschine gestellt haben. Auch die Browser-Konkurrenz Netscape mit ihrem Produkt Navigator verrät durch die Cookies einiges: In der entsprechenden Datei findet sich eine Liste mit allen besuchten Internet-Seiten, die Cookies verwenden – das sind heute praktisch alle kommerziellen Seiten.

Oder auf der Festplatte findet sich beispielsweise eine Datei karl.pick@amazon.de.txt. Dies lässt jeden, der Zugriff auf Ihren Rechner hat, erkennen, dass Herr Pick die Website amazon.de aufgerufen hat. Und wenn man diese Dateien öffnet - das

funktioniert im Allgemeinen durch einen einfachen Doppelklick - offenbaren sie oft noch viel mehr Details.

Diese Art der Protokollierung des Surf-Verhaltens lässt sich recht einfach unterbinden. Weder der Browser noch die Internet-Seiten nehmen es Ihnen übel, wenn Sie die Dateien einfach löschen. Im schlimmsten Falle werden Sie beim nächsten Besuch der Internet-Seite nicht wiedererkannt.

Um in Zukunft diese Methode der Surfkontrolle zu umgehen, können Sie in allen Browsern das Schreiben von Cookies unterbinden – vorausgesetzt Ihr/-e Systemadministrator/-in hat Ihnen nicht das Recht entzogen, diese Einstellungen zu ändern.

## 9.2. Löschen von Cookies

Im **Internet-Explorer** gehen Sie dazu folgendermaßen vor:

- Starten Sie den Explorer mit jeder beliebigen Seite (die Startseite ist so gut wie jede andere)
- Klicken Sie auf Extras
- Klicken Sie auf Internetoptionen
- Klicken Sie auf Cookies Löschen
- Klicken Sie auf Dateien Löschen
- Klicken Sie auf Verlauf leeren

## 9.3. Anlegen von Cookies verbieten

Sie können das Anlegen von Cookies in Zukunft verbieten bzw. einschränken.

Im **Internet-Explorer** gehen Sie dazu folgendermaßen vor:

- Starten Sie den Explorer mit jeder beliebigen Seite (die Startseite ist so gut wie jede andere)
- Klicken Sie auf Extras
- Klicken Sie auf Internetoptionen
- Setzen Sie die Tage die Seiten im Verlauf aufbewahrt werden sollen auf 0
- Klicken Sie auf Einstellungen
- Setzen Sie die Größe des Speichers für temporäre Internetdateien auf 0

Beachten Sie dabei jedoch, dass manche Internet-Seiten dann nicht mehr einwandfrei funktionieren. Wenn Sie auf solche Seiten angewiesen sind, empfiehlt es sich, die

Dateien lieber von Zeit zu Zeit zu löschen, als sie generell zu verbieten. Dann werden Sie schlimmstenfalls beim nächsten Besuch der Seite nicht wiedererkannt. Dann hilft nur, regelmäßig die genannten Dateien zu löschen. Vergessen Sie aber nicht, dass Ihr Sysadmin dennoch zahlreiche Möglichkeiten hat Ihr Surfverhalten zu beobachten, die durch das Abschalten der Cookies nicht verhindert werden können.

Ein wenig eleganter geht es mit so genannten Paranoia-Programmen, wie z.B. „Internet-Cleanup“ der Firma Ontrack (<http://www.ontrack.de>) oder kostenlosen Programmen aus dem Internet, die Ihnen das Löschen von verräterischen Protokollen und Cookies abnehmen. Vorausgesetzt natürlich Sie dürfen diese Programme auf Ihrem Arbeitsplatz-Rechner installieren, was oft nicht erlaubt ist.

---

**Sprechen Sie in jedem Fall vorher mit Ihrem Betriebsrat!**

---

## **9.4. Wie man Cookies findet, wie man sie sich ansehen kann und wie man sie verbietet**

Unter **Windows XP** legt der Internet-Explorer die Cookies standardmäßig im Verzeichnis C:/Dokumente und Einstellungen/"Benutzername"/cookies ab. Für jedes Cookie wird dabei eine eigene Datei erzeugt.

**Modzilla oder Firefox-Browser** legen die Cookies im Benutzerverzeichnis in einer einzigen Datei namens cookies.txt ab, Dabei wird hier nur eine einzige Datei mit dem Namen cookies.txt angelegt, in der alle Einträge untereinander aufgelistet sind.

**Wenn Sie auf Ihrer Festplatte das Verzeichnis nicht finden, können Sie leicht danach suchen:**

Starten Sie den Windows-Explorer, gehen Sie auf Laufwerk C: und drücken Sie F3 (für „Suche nach Dateien und Ordnern“). Geben Sie als zu suchenden Namen \*cookies.txt\* ein. So werden Sie schnell entweder die Datei selbst oder aber den entsprechenden Ordner finden.

Um das Anlegen von Cookies in Zukunft zu verbieten oder einzuschränken, wählen Sie zum Beispiel bei Mozilla oder Firefox-Browsern im Menüpunkt „Bearbeiten“ den Eintrag „Einstellungen“ aus. Klicken Sie dort auf „Erweitert“. Jetzt sehen Sie rechts die Möglichkeiten, wie Sie in Zukunft mit Cookies umgehen können.

Im **Internet-Explorer** finden Sie die entsprechenden Einstellungen unter „Extras“,

„Internetoptionen“, „Datenschutz“ und dann den Schalter „Erweitert“. In den beiden genannten Menüs finden Sie außerdem noch jede Menge anderer interessanter Einstellungen zu Datensicherheit und zum Datenschutz.

Leider können wir nur einige Browser beispielhaft anführen, da eine vollständige Auflistung den Rahmen unserer Broschüre sprengen würde.

## 9.5. Akzeptanz von Cookies

Bei den Browsern (z.B. Internet Explorer oder Netscape) lässt sich einstellen, ob Cookies akzeptiert und ob zusätzlich Warnmeldungen angezeigt werden sollen. So erhalten Sie einen Überblick darüber, wer bei zukünftigen Web-Kontakten zusätzliche Informationen aus Cookies beziehen kann.

Einstellen der Cookie-Akzeptanz im Netscape: unter „Bearbeiten“, „Einstellung“, „Erweitert“, im Internet Explorer: unter „Extras“, „Internetoptionen“, „Datenschutz“, „Erweitert“

## 9.6. Ansehen der vorhandenen Cookies

Wenn Sie den Microsoft **Internet-Explorer** auf einem Windows-Betriebssystem verwenden, können Sie ganz einfach nachsehen, was im Moment so alles über Sie gespeichert ist:

- 1) Öffnen Sie ein neues Browser-Fenster (Im Menü über „Datei / Neu / Fenster“)
- 2) Geben Sie in dieses Fenster in der Adresszeile folgendes ein:  
files://%userprofile%/Cookies/(kein „http://“ davor, auch kein „www“ o.ä.)  
und drücken Sie die Return-Taste.

In dem Fenster werden jetzt alle Cookies auf Ihrem Rechner dargestellt. Meistens können Sie sich die Inhalte durch einen einfachen Doppelklick anzeigen lassen - aber schon die Namen der Dateien sind sehr viel sagend.

## 10. Cache free – Der „Verlauf“ der „Historie“

In vielen Fällen speichern Anwendungen Informationen in Form von Dateien auf der lokalen Festplatte, um durch das Zwischenspeichern Ressourcen von abgerufenen Inhalten aus dem Internet zu schonen bzw. um die Ladezeiten zu verkürzen. Dieses Verfahren nennt man „Cachen“ und es ist durchaus sinnvoll.

Im sog. Cache werden besuchte Internetseiten zwischengespeichert, um bereits abgerufene Informationen schneller aufrufen zu können. Dadurch erhöht sich zwar die Ladegeschwindigkeit beim Surfen, es kann jedoch auf einfache Weise auch nachvollzogen werden, welche Websites Sie besucht haben. Die gespeicherten Dateien geben also genaue Auskunft über Ihr Verhalten im Internet wieder, da sie im „Klartext“ oder „Klarbild“ für jeden, der Zugriff auf die Festplatte hat, lesbar sind.

Auch die so genannte „History-List“, manchmal auch als „Verlauf“ oder „Historie“ bezeichnet, sagt jedem, der Zugriff auf Ihren Rechner hat, welche Internet-Seiten Sie in den letzten Tagen oder Wochen besucht haben.

---

**Und wieder können Sie von jedem/jeder, der Zugriff auf Ihren Rechner hat, ohne Probleme angesehen werden.**

---

Ähnlich wie bei den Cookies können Sie sich auch gegen das Zwischenspeichern im Cache sehr einfach schützen. Sie können die Caches ausschalten. Allerdings geht dann das Surfen viel, viel langsamer, so dass es sich auch hier empfiehlt, den Cache einfach gelegentlich zu löschen.

### 10.1. Ansehen des Caches

Wenn Sie den Microsoft **Internet-Explorer** auf einem Windows-Betriebssystem verwenden, können Sie ganz einfach nachsehen, was im Moment so alles über Sie gespeichert ist:

- 1) Öffnen Sie ein neues Browser-Fenster (Im Menü über „Datei / Neu / Fenster“)
- 2) Geben Sie in dieses Fenster in der Adresszeile folgendes ein:  
files://%userprofile%/Lokale Einstellungen/Temporary Internet Files/(kein „http://“ davor, auch kein „www“ o.ä.) und drücken Sie die Return-Taste.

In dem Fenster wird jetzt der gesamte Cache auf Ihrem Rechner dargestellt. Sie können sich die Inhalte (beispielsweise die Grafiken, aber auch die HTML-Dateien) durch einen einfachen Doppelklick anzeigen lassen.

## 10.2. Den Cache finden, ansehen und löschen

Unter **Windows XP** legt der **Internet-Explorer** alle gecachten Dateien standardmäßig im Verzeichnis C:/Dokumente und Einstellungen/Lokale Einstellungen/Temporary Internet Files/ ab.

**Modzilla oder Firefox-Browser** legen den Cache in einem Directory namens „Cache“ ab. Der Inhalt wäre zu löschen.

Wenn Sie auf Ihrer Festplatte das Verzeichnis nicht finden, können Sie leicht danach suchen: Starten Sie den **Windows-Explorer**, gehen Sie auf Laufwerk C: und drücken Sie F3 (für „Suche nach Dateien und Ordnern“). Geben Sie als zu suchenden Namen \*cache\* oder eventuell \*temporary\* ein. So werden Sie schnell den entsprechenden Ordner finden. Das Ansehen der Dateien funktioniert im Allgemeinen wieder durch einen einfachen Doppelklick.

Die Einstellungen des Caches können Sie in den gleichen Menüs wie die der Cookies ändern: In Netscape unter „Bearbeiten“, „Einstellungen“, „History“, „Erweitert“, „Cache“, im Internet-Explorer unter „Extras“, „Internetoptionen“, „Allgemein“ und dann „Einstellungen“.

## 10.3. Beeinflussen Sie den Verlauf der Geschichte

### – Ihre History

Sie kennen - und mögen - sicher die Funktion Ihres Internet-Browsers, dass er Ihre Eingaben von Links automatisch ergänzt.

Wenn Sie beispielsweise die Seite <http://www.interesse.at/it> zu einem späteren Zeitpunkt noch einmal besuchen, reicht es im Allgemeinen aus, die ersten paar Buchstaben einzugeben. Ihr Browser vervollständigt sie dann automatisch.

Damit das funktioniert - und auch aus ein paar anderen Gründen -, muss er sich aber „merken“, welche Seiten Sie schon alles besucht haben. Dafür speichert er eine Verlaufsliste oder auch „Historie“ genannt.

In dieser Historie stehen alle Seiten, die Sie in den letzten Tagen, Wochen oder gar Monaten besucht haben.

## 10.4. Die Verlaufsliste finden, anzeigen, löschen

Öffnen Sie ein neues Browserfenster. Löschen Sie dann alles aus der Adressleiste und klicken Sie rechts an der Adressleiste auf den Pfeil nach unten. Jetzt sehen Sie die zuletzt besuchten Seiten.

**Viel zu wenig Einträge?**

Dann geben Sie mal „a“ in der Adresszeile ein und klicken Sie wieder auf den Pfeil. Jetzt sehen Sie alle Internet-Seiten, die Sie in letzter Zeit besucht haben und die mit „a“ beg/-innen.

Wenn Sie den **Microsoft Internet-Explorer** auf einem Windows-Betriebssystem verwenden, geht es auch noch ein wenig übersichtlicher:

- 1) Öffnen Sie ein neues Browser-Fenster (Im Menü über „Datei / Neu / Fenster“)
- 2) Geben Sie in dieses Fenster in der Adresszeile folgendes ein:  
files://%userprofile%/Lokale Einstellungen/Verlauf/ (kein „http://“ davor, auch kein „www“ o.ä.) und drücken Sie die Return-Taste.

In dem Fenster können Sie jetzt Ihre Internet-Aktivitäten der letzten Tage nachvollziehen - fein ordentlich nach Wochentagen sortiert - und die Seiten per Doppelklick auch noch einmal besuchen.

### Verlaufsliste löschen/ausschalten

Verlaufsliste löschen/ausschalten - so funktioniert's:

In **Netscape**: unter „Bearbeiten“, „Einstellungen“, „History“

Im **Internet-Explorer**: unter „Extras“, „Internetoptionen“, „Allgemein“

### Unsichtbare Spione

Neben diesen „Standard-Protokollen“ gibt es bei modernen Betriebssystemen noch jede Menge weitere Dateien, in denen das Benutzerverhalten aufgezeichnet wird. Oftmals wie gesagt zur Aufrechterhaltung des Betriebs - was ja auch sinnvoll erscheint - und nicht für etwaige Überwachungs-Zwecke.

Weniger sinnvoll hingegen erscheint, dass Benutzer/-innen und Benutzer – auch Profis – von dieser Kontrolle in aller Regel nichts wissen und keinen Einfluss auf Art, Umfang und Gültigkeit haben.

Gegen diese Protokollierungen kann man sich im Allgemeinen nicht wehren, selbst wenn es noch so sehr von allen Beteiligten gewünscht ist.

Um zu erfahren, was der PC so alles mitprotokolliert, hilft oft nur das gelegentliche Suchen nach veränderten Dateien auf der lokalen Festplatte.

In Windows kann man mit der Suchfunktion (Start \_ Suchen \_ Datei/Ordner) alle veränderten Dateien in einem bestimmten Zeitraum anzeigen lassen.

Durch das bloße Anschauen der Dateinamen kommt man oft dahinter, welche Anwendung welche Aktivitäten aufzeichnet. Besonders „verdächtig“ sind Dateien

mit den Endungen .log oder .dat, und oft lohnt es sich, einen Blick hineinzuworfen – wieder mit einem gewöhnlichen Texteditor oder Schreibprogramm.

### **Aber Vorsicht:**

Viele der Dateien, die Sie finden werden, sind Systemdateien, in denen Informationen abgespeichert werden, die nichts mit einer Überwachung zu tun haben und die keinesfalls geöffnet, geändert oder gelöscht werden dürfen! Und selbst wenn Sie entdecken, dass Ihre (Online-) Aktivitäten protokolliert werden, sollten Sie diese Dateien in aller Regel nicht löschen oder verändern, da Sie damit im Zweifelsfall das entsprechende Programm durcheinander bringen!

Erkundigen Sie sich im Einzelfall lieber beim Systemadmin oder in der Fachwelt, warum diese Protokolle geschrieben werden, ob man sie abschalten kann oder ob man sie zumindest so absichern kann, dass niemand mehr Zugriff darauf hat. Oftmals haben sie nämlich für die Systemadministration keinen wirklichen Nutzen und ausgewertet werden sie ohnehin nur in den seltensten Fällen.

## **II. Spionageprogramme**

Ganz anders als bei den bisher genannten mehr oder weniger ausführlichen Protokollierungen und Zwischenspeichern, die meist automatisch vom System vorgenommen werden (müssen), verhält es sich mit Spionage-Programmen auf den Arbeitsplatz-Rechnern.

Diese müssen mit Vorsatz installiert werden, werden im Allgemeinen regelmäßig ausgewertet oder überwacht und kosten zudem meistens noch Geld, was nahe legt, dass Sie durch ihren Einsatz letztendlich irgendwie wieder Geld sparen sollen.

Spionage-Programme werden mit Vorsatz auf der Festplatte installiert, um Ihr Surfverhalten regelmäßig auswerten und überwachen zu können. Sie laufen ständig im Hintergrund mit und zeichnen mitunter sämtliche Tastaturfolgen auf - also alle Daten, die der Anwender über die Tastatur eingibt. Die gesammelten Daten werden später unbemerkt an den/die Systemadministrator/-in weitergeschickt.

---

**Viele Programme können inzwischen aber weit mehr, als nur die gedrückten Tasten aufnehmen:**

---

Über eine Assoziation der gedrückten Taste mit dem Programm, das gerade aktiv ist, lassen sich auch gezielte Aktionen nachvollziehen: Ihre Aktivitäten im Chat, Ihre Kennwörter, oder einfach Ihre Briefe in Word, auch wenn Sie sie nicht gespeichert haben.

Oftmals machen solche Programme in regelmäßigen Abständen auch noch Fotos Ihres Bildschirm - somit kann nachher wie in einem Video nachvollzogen werden, was Sie so den ganzen Tag gemacht haben.

Und ganz dreiste Programme schalten sogar heimlich noch eine eventuell vorhandene WebCam oder ein Mikrofon ein und nehmen auch noch Ihre Reaktion vor dem Rechner mit auf.

---

**Da die spezielle Software automatisch im Hintergrund mitläuft, ist sie für einen Laien nur schwer zu entdecken.**

---

Da nur die wenigsten Anwender/-innen in der Lage sein dürften „ungewöhnliche“ Aktivitäten Ihres PCs richtig zu interpretieren (ungewöhnliche Festplattengeräusche, regelmäßige „Hänger“ etc.) und kaum jemand das Wissen und die Lust hat, regelmäßig seine Festplatte auf „ungewöhnliche“ Dateien zu durchsuchen, gibt es für einige der weit verbreiteten Spionage-Programme auch spezielle Software zum Aufdecken solcher Spionage-Programme, die ähnlich wie Virencans funktionieren.

Allerdings sind diese Programme ganz speziell auf einzelne Spionage-Anwendungen zugeschnitten, und da der Markt an Spionage-Software rasant wächst und die Anzahl der unterschiedlichen Programme inzwischen recht unübersichtlich ist, helfen sie meist nur wenig. Ein Test kann trotzdem nicht schaden!

---

**Wie man Spionagesoftware erkennen kann**

---

Eigentlich fast gar nicht...

Abgesehen von solchen Programmen, die durch die Spionage-Abwehr-Software erkannt werden, kann man sie kaum entdecken.

Sinnvoll ist es auf jeden Fall gegenüber „unnötigen“ Geräten am PC misstrauisch zu sein:

- 1) Hat ihr PC eine WebCam und Sie haben Sie noch nie benutzt? Dann drehen Sie sie doch einfach in eine Richtung, wo sie nichts zu sehen hat. Oder stellen Sie einen Gegenstand vor das Objektiv. Ein vorhandenes Lämpchen, das normalerweise an ist, wenn die Kamera in Betrieb ist, ist kein sicherer Anhaltspunkt, dass sie wirklich aus ist: Diese Lämpchen lassen sich über die Software auch bei eingeschalteter Kamera ausschalten.
- 2) Hat Ihr PC ein Mikrofon, das sie nicht brauchen? Dann ziehen Sie doch einfach den Stecker (oder lassen ihn von Ihre(m)/-r Administrator/-in ziehen).

Ansonsten kann man Spionagesoftware nur mit einigem technischen Wissen bekommen:

3) Nach „ungewöhnlichen“ Dateien suchen - also beispielsweise solchen, die sich andauernd verändern und größer werden (das könnte eine Protokoll-Datei für irgendetwas sein) - aber bitte keinesfalls einfach löschen!!! Damit können Sie die Funktion des Systems beeinträchtigen.

### **Auf „ungewöhnliche“ Aktivitäten achten:**

Macht Ihr Rechner alle 1 oder 2 Minuten grundlos eine kurze Pause, ohne dass eines der verwendeten Programme gerade etwas tut - das merkt man oftmals daran, dass die Maus einfach hängen bleibt? Dann könnte eine Spionage-Software am Werk sein. Aber meistens sind es nur ganz unkritische Aktionen, z.B. das automatische Abrufen der Mails bei Outlook, die automatische Zwischenspeicherung von Word etc.

## **11.2. Tastensammler**

„**Key-Logger**“ ist der Überbegriff für Programme, die alle Aktivitäten auf einem PC mitprotokollieren.

Es gibt sie in unterschiedlichen Ausprägungen und mit verschiedenen Protokollierungstiefen, beispielsweise für Privathaushalte als „CyberSitter“ oder auch für Unternehmen mit zentraler Auswertungsmöglichkeit der überwachten Arbeitsplatzrechner.

### **Das Grundprinzip der Key-Logger ist dabei sehr einfach:**

Es wird jeder einzelne Tastendruck, der auf einem Rechner gemacht wird, aufgezeichnet. Dadurch lässt sich jede Aktivität nachvollziehen, insbesondere auch die Eingabe von Kennwörtern. Zusätzlich zu dieser Tastaturbeobachtung werden von manchen Key-Loggern auch noch in kurzen Abständen Bildschirmfotos („Screenshots“) gemacht und auf der Festplatte abgelegt, so dass die PC-Aktivitäten wie mit einem Videofilm nachvollzogen werden können.

Die Kernfunktion von Key-Loggern, also die Tastenprotokollierung, kann auf vielfältige Weise geschehen. Beispielsweise gibt es dafür auch spezielle Hardware, also ein kleines Gerät, das ganz einfach direkt am Tastatur-Stecker angeschlossen wird. Dieses Gerät zeichnet alle Tastaturaktivitäten auf und kann zu einem späteren Zeitpunkt ausgelesen werden.

Allerdings können solche Hardware-Eingriffe im Allgemeinen sehr schnell entdeckt werden, indem man einfach das Tastaturkabel verfolgt und nachsieht, ob sich irgendein ungewöhnliches Gerät daran befindet.

## Viel eleganter geht es mit Software.

Diese Software muss auf dem Rechner bewusst installiert werden (beispielsweise durch den/die Systemadministrator/-in) und läuft ab dann automatisch im Hintergrund ab. Meist ist sie noch dazu sehr gut geschützt und kann nicht mit einfachen Mitteln entdeckt werden (sie steht also weder in der Task-Liste noch hinterlässt sie leicht erkennbare Spuren auf der Festplatte). Die verschiedenen Softwareprodukte, die weiter unten auch einzeln beschrieben sind, unterscheiden sich neben der Menge an aufgezeichneten Informationen beispielsweise auch in der Art, diese Informationen auszuwerten.

Viele Programme liefern einfach nur die gedrückten Tasten als eine lange Zeichenkette zurück – entsprechend mühsam ist dann auch das Auswerten. Andere Programme ordnen die Tastatureingaben automatisch den geöffneten Anwendungen zu, so dass bei den Protokollen beispielsweise sehr einfach zwischen Internet-Browser, E-Mail-Programm oder Online-Chat unterschieden werden kann und übliche Anwendungen wie Textprogramme ganz ignoriert werden.

Es gibt auch große Unterschiede, was mit diesen gesammelten Daten passiert: Manche Programme schreiben sie einfach nur in eine Datei auf der lokalen Festplatte. Manche legen sie auf einem zentralen Server im Netzwerk ab. Wieder

andere verschicken sie per E-Mail automatisch an Administratoren/-innen oder Vorgesetzte.

Einige dieser Funktionen können beispielsweise auch nur durch bestimmte Aktionen ausgelöst werden. So gibt es Programme, die bei der Eingabe einer „bösen“ URL oder beim Tippen bestimmter Worte in das E-Mail-Programm automatisch eine Mail an den/die Administrator/-in verschicken, ansonsten aber keine Protokolle mitschreiben.

Interessant ist, dass fast alle Hersteller von Key-Logger-Programmen angeben, die Software in erster Linie gar nicht für die Überwachung von Unternehmens-Arbeitsplätzen entwickelt zu haben, sondern für Privathaushalte.

Weniger überraschend ist, dass die meisten Programme dieser Art in den USA entwickelt werden und zum Teil noch gar nicht auf dem deutschen Markt erhältlich sind. Nach Angaben der Hersteller war oftmals die Überwachung des Surfverhaltens von Kindern am heimischen PC oder des E-Mail-Verkehrs des potenziell untreuen Ehepartners das primäre Ziel. Die Verkaufszahlen aber belegen, dass viele der Programme überwiegend von Unternehmen gekauft werden und dass die Anzahl der mit solcher Software überwachten Arbeitsplätze dramatisch zunimmt.

Nur ein Beispiel: Ein in den USA bereits seit einiger Zeit bekanntes und inzwischen auch in Deutschland offiziell verfügbares Programm namens „Spector“ der Firma ProtectCom, das eigentlich für private Anwendungen entwickelt wurde, wurde bereits vor dem offiziellen Marktstart in Deutschland am 23. April 2001 1.000 mal lizenziert, davon über 500 an Firmen.

Bereits im September waren in Deutschland rund 4.500 Installationen vorhanden, mit einer Verschiebung der Unternehmensnutzung hin zu 75%. Weltweit wurde Spector – nur ein Programm von vielen! – bisher über 70.000 Mal verkauft.

Die verbreitetsten Programme aus der Kategorie Key-Logger sowie ihre Besonderheiten sind folgende:

### **11.3. Produktinformation zu Spionagesoftware**

---

**Spector ProtectCom**  
([www.spectorsoft.de](http://www.spectorsoft.de))

---

Ursprünglich in den USA für den privaten Markt entwickelt. Inzwischen auch in Deutschland verfügbar (über 5.000 Installationen) und überwiegend in Unternehmen eingesetzt.

Protokolliert:

- Alle Tastenanschläge,

- alle besuchten Internet-Seiten,
- alle Chat-Unterhaltungen,
- alle Mails und Instant-Messaging-Aktivitäten (ICQ, MS-Messenger etc.),
- alle Bildschirmmasken (Screenshots) mit Wiedergabefunktion als „Videofilm“ und automatischer Analyse der Bilder.
- Läuft wahlweise im sichtbaren oder unsichtbaren Modus.
- Speicherung der Protokolle und Bilder auf der lokalen Festplatte.
- Durch die Hinterlegung von Schlüsselwörtern und Phrasenlisten kann bei Eingabe der entsprechenden Wörter eine automatische E-Mail generiert werden („Alarmpfunktion“).
- Ausgezeichnet mit dem „BigBrother Award 2001 für Überwachung am Arbeitsplatz“.
- Preis: ca. 75 € pro Installation.

---

**PC-Spion G-Data**  
([www.gdata.de](http://www.gdata.de))

---

In Deutschland vorwiegend für den privaten Markt entwickelt.

Protokolliert:

- Alle Tastenanschläge,
- alle besuchten Internet-Seiten,
- alle Bildschirmmasken (Screenshots).
- Läuft wahlweise im sichtbaren oder unsichtbaren Modus.
- Speicherung der Protokolle und Bilder auf der lokalen Festplatte.
- Kann zusätzlich administrativ in den Rechner eingreifen: Laufwerke oder Ordner ausblenden, zeitliche Zugangsbeschränkung und anderes.
- Preis: ca. 40 € pro Installation.

---

**STARR IOpus**  
([www.iOpus.com/de/](http://www.iOpus.com/de/))

---

In zwei unterschiedlichen Versionen für Privatanwender und Unternehmen (Pro-Version) erhältlich.

Protokolliert:

- Alle benutzen Programme,
- alle Tastatureingaben,
- alle besuchten Internet-Seiten,
- alle Bildschirmmasken (Screenshots) mit automatischer Analyse der Bilder.
- Die Log-Datei kann automatisch per E-Mail verschickt oder regelmäßig auf einen zentralen Server überspielt werden (Pro-Version).
- Kann im Netzwerk ferninstalliert werden (Pro-Version).
- Auswertung der Protokolle in HTML-Ansicht, Excel-Format oder als Rohdaten.
- Speicherung der Protokolle und Bilder auf der lokalen Festplatte (bei der Pro-Version nur temporär).
- Preis: ca. 70 € pro Installation.

.....  
**Investigator WinWhatWhere**  
**([www.winwhatwhere.com](http://www.winwhatwhere.com))**  
.....

Überwiegend für den Einsatz in Unternehmen entwickelt.

Protokolliert:

- Alle Tastatureingaben,
- alle Bildschirmmasken (Screenshots),
- Inhalte aus Bildern („Windows Content“),
- alle Dateioperationen.
- Kann auf Wunsch mit einer Web-Cam kombiniert werden, um den entsprechenden Log-Einträgen auch Bilder des Benutzers zuzuordnen.
- Kann im Netzwerk ferninstalliert werden.
- Die Log-Datei kann automatisch per E-Mail verschickt werden.
- Läuft wahlweise im sichtbaren oder unsichtbaren Modus.
- Versteckt sich selbst durch Verschieben und Umbenennen, um nicht auf dem PC erkannt zu werden.
- Durch die Hinterlegung von Schlüsselwörtern und Phrasenlisten kann bei Eingabe der entsprechenden Wörter eine automatische E-Mail generiert werden („Alarmfunktion“).

- Temporäre Speicherung der Protokolle und Bilder auf der lokalen Festplatte.
- Preis pro Installation: ca. 25 € (bei mehr als 500 Lizenzen) bis zu 110 € (Einzelplatz).

**Insight Trisys Inc.**  
 ([www.trisys.com](http://www.trisys.com))

Überwiegend für den Einsatz in Unternehmen entwickelt.

Protokolliert:

- Alle verwendeten Programme inkl. Zeitraum und Dauer, in dem das Programm benutzt wurde,
- alle im Internet-Explorer aufgerufenen Seiten (nicht von anderen Browsern!).
- Speichert alle Aktivitäten zentral auf einem Server oder sogar direkt bei Trisys auf speziellen Servern.
- Die Auswertung kann „online“ über ein Web-Frontend erfolgen.
- Preis pro Installation: ab ca. 12 €.

**KeyGhost Orth Sicherheitstechnik**  
 ([www.keyghost.de](http://www.keyghost.de))

Hardware, die zwischen die Tastatur und den PC gesteckt oder in der Tastatur eingebaut wird.

- Protokolliert jeden Tastendruck.
- Speichert bis zu 2.000.000 Zeichen, die aus dem Speicher dann wiedergegeben werden können.
- Preis pro Gerät: zwischen 160 € und 520 €.

**WinGuardian Webroot Software**  
 ([www.webroot.com](http://www.webroot.com))

Überwiegend für den Einsatz in öffentlichen Einrichtungen (Bibliotheken, Schulen etc.) entwickelt.

Protokolliert:

- Alle verwendeten Programme,

- alle besuchten Internet-Seiten,
- alle Tastenfunktionen,
- alle Bildschirmmasken (Screenshots).
- Optional kann ein „Zustimmungs-Modus“ eingeschaltet werden, bei dem der Benutzer über die Protokollierung aufgeklärt wird und diese explizit bestätigen muss.
- E-Mail-Versand der Log-Protokolle möglich.
- Speichert die Daten auf der lokalen Festplatte.
- Netzwerkfähig.
- Preis pro Installation: ab ca. 45 €.

---

**IamBigBrother**  
 ([www.iambigbrother.com](http://www.iambigbrother.com))

---

Überwiegend für den Einsatz im privaten Bereich entwickelt.

Protokolliert:

- Alle verwendeten Programme,
- alle besuchten Internet-Seiten,
- alle E-Mails,
- alle Tastenfunktionen,
- alle Bildschirmmasken (Screenshots).
- Bietet zusätzlich eine Filter-Funktion, mit welcher der Aufruf von festgelegten Internet-Seiten gleich unterbunden werden kann.
- Speichert die Daten auf der lokalen Festplatte.

## 11.4. Was kann ich tun?

Die Hersteller von Key-Logger-Programmen geben sich größte Mühe, ihre Programme zu verstecken.

Fast alle Key-Logger können im sogenannten Stealth- oder auch Silent-Mode betrieben werden, in dem sie dann nicht auf den ersten Blick erkennbar sind, da sie beispielsweise nicht in der Task-Liste von Windows auftauchen. Auch verraten sie sich im Allgemeinen nicht durch andere Ereignisse, die den/der Benutzer/-in aufmerksam machen könnten (vielsagende Dateinamen, Tray-Icons, Popup-Fenster etc.). Am Besten versteckt sich wohl noch das Programm „Investigator“ von

WhinWhatWhere. Es wechselt in unregelmäßigen Abständen selbstständig den Namen und den Speicherort und macht es damit dem Benutzer sehr schwer, gezielt nach ihm zu suchen.

---

**Zum Aufspüren einiger dieser Programme gibt es bereits spezielle Software, die ähnlich den handelsüblichen VirenScannern arbeitet.**

---

Das sind insbesondere die beiden Programme „Elbtecsan“ und „Antispector“ – beide sind im Internet kostenlos verfügbar.

Elbtecsan und AntiSpector sind speziell dazu da, das weiter oben vorgestellte Programm Spector der Firma ProtectCom sowie das technisch sehr ähnliche Programm eBlaster der gleichen Firma zu entdecken. In wenigen Sekunden hat man somit Gewissheit, ob der eigene Rechner von Spector überwacht wird. Für den Fall, dass man nicht berechtigt ist, Programme herunterzuladen und auszuführen, gibt es zusätzlich auf der gleichen Internet-Seite auch eine Online-Version des Tests.

Leider wurde die Firma ElbTec aufgelöst. Das Programm Elbtecsan finden Sie noch in einschlägigen Portalen.

z.B. unter <http://www.download.trampelpfad.de>

Die Angst vor Spector scheint groß zu sein, denn innerhalb eines halben Jahres wurde die Software rund 300.000 Mal heruntergeladen.

Ähnlich wie Elbtecsan sucht auch der Antispector speziell nach der Spector-Software. Dieses Programm gibt es ebenfalls kostenlos unter <http://www.trojancheck.de/antispector.html>.

Aber auch Key-Logger, für die bisher keine speziellen Gegenmittel entwickelt wurden, lassen sich meist mit sehr einfachen Mitteln und ein wenig Bereitschaft, den eigenen PC besser zu verstehen, ausfindig machen.

Mit Ausnahme des Programms „Insight“ von Trisys legen alle Key-Logger die gesammelten Daten und Bildschirmfotos zumindest zeitweise auf der lokalen Festplatte ab. Damit sind sie ähnlich leicht zu entdecken wie die weiter oben erwähnte allgemeinen Log-Protokolle.

Wer sich unsicher fühlt, ob er/sie überwacht wird, sollte sich von Zeit zu Zeit die kürzlich (!) veränderten Dateien auf der lokalen Festplatte ansehen (Start \_ Suchen \_ Datei/Ordner). Auch hier sind insbesondere wieder Dateien mit den Endungen wie .log oder .dat verdächtig.

Allerdings bieten einige der oben genannten Programme auch die Möglichkeit, Log-Protokolle verschlüsselt abzulegen, so dass sie nicht mit normalen Texteditoren oder Textprogrammen angesehen werden können.

In diesen Fällen hilft es vielleicht weiter, die verdächtigen Dateien ein wenig zu beobachten: Merken Sie sich beispielsweise die genaue (!) Größe der Datei (im Windows-Explorer mit der rechten Maustaste auf die entsprechende Datei klicken und „Eigenschaften“ auswählen), öffnen sie dann beispielsweise in ihrem Internet-Browser eine neue Internet-Seite und schauen Sie sich dann sofort wieder die verdächtige Datei an. Wenn Sie sich in der Größe verändert hat (oft nur um wenige Byte), ist das schon ein deutliches Zeichen!

### **Aber auch hier gilt wieder:**

Vorsicht! Nicht jede Datei, die sich oft verändert, muss unbedingt ein Protokoll sein! Daher sei hier die Warnung wiederholt, dass viele der Dateien, die Sie finden werden, Systemdateien sind, in denen Informationen abgespeichert werden, die nichts mit einer Überwachung zu tun haben und die keinesfalls geöffnet, geändert oder gelöscht werden dürfen!

Wenn Sie sich unsicher sind, ob Sie überwacht werden, erkundigen Sie sich im Einzelfall lieber in der Fachwelt wie beispielsweise den Newsgroups oder den einschlägigen Datenschutz-Seiten was es mit diesen speziellen Dateien auf sich hat. Manchmal können Sie auch die Bildschirm-Abzüge (Screenshots), die von Key-Loggern gemacht werden, auf der lokalen Festplatte finden. Suchen Sie dazu beispielsweise nach Dateien mit der Endung .gif, .jpg, .png oder .tif, die kürzlich verändert wurden. Wenn Sie solche Dateien finden, reicht meist ein Doppelklick, um sie sich im vom Betriebssystem mitgelieferten Bildbetrachter anzusehen.

---

**Achtung: In den weiter oben genannten Cache-Verzeichnissen der Internet-Browser (z.B. netscape\users\Benutzername\Cache\ oder c:\windows\Temporary Internet Files) werden Sie jede Menge von neuen .gif und .jpg Dateien entdecken. Diese sind nicht unbedingt verdächtig, da sie ja nur der Cache des Browsers sind, aber das Öffnen des einen oder anderen Bildes kann nicht schaden. Sie werden überrascht sein, wie gut Sie auch unabsichtlich überwacht werden.**

---

## 12. Die zentrale Überwachung – Firewalls, Router, Proxy

Einen ganz anderen Ansatz zur Überwachung liefern die zentralen Verbindungen der Unternehmensnetzwerke mit dem Internet.

Wie eingangs erläutert, findet der gesamte Datenaustausch eines Unternehmens mit dem Internet – egal ob E-Mail, WWW oder anderes – über ein oder mehrere zentrale Gateways statt. Diese Gateways haben die Aufgabe, Informationen zu „routen“, also zu bestimmen, auf welchen Rechner die Informationspakete weitergereicht werden – unternehmensintern oder -extern. Dazu muss jedes einzelne Datenpaket „geöffnet“, die Zieladresse daraus analysiert (die sogenannten IP-Adresse, die einen Rechner in einem Netzwerk eindeutig bestimmt) und das Paket dann anschließend an den entsprechenden Rechner weitergereicht werden. Nichts ist also leichter, als diese Informationen irgendwo abzuspeichern!

Die hier abstrakt als „Gateways“ bezeichneten Programme haben im Allgemeinen noch andere (zusätzliche) Funktionalitäten und auch andere Namen und oftmals kommen viele dieser Geräte gleichzeitig zum Einsatz – nicht aus Gründen der Überwachung, sondern um das Unternehmensnetzwerk zu managen.

### 12.1. Firewalls

Sind in erster Linie dazu da, den Datenverkehr im Unternehmensnetzwerk vor Angriffen aus dem Internet zu schützen. Dazu können Regeln festgelegt werden, welche Art von Informationen oder Diensten in das Unternehmensnetzwerk hereingelassen werden und welche es verlassen dürfen. Beispielsweise wird über Firewalls geregelt, ob ein/-e Benutzer/-in aus dem Internet Programme herunterladen darf, ob er/sie überhaupt ins Internet oder vielleicht nur in das Intranet darf, und wie bei Verstößen gegen diese Regeln zu verfahren ist. Dazu ist es selbstverständlich notwendig, dass jede (!) Anforderung an das Internet durchsucht wird.

### 12.2. Router

Sind technisch unabdingbare Geräte (oder Software-Lösungen), die entscheiden, welche Informationen in welches Netzwerk (intern oder extern) weitergereicht werden. Dazu wird – wie oben beschrieben – jedes Datenpaket auf seine Herkunft und sein Ziel untersucht und entsprechend weitergeleitet.

### 12.3. Proxy-Server

Weiter oben wurde der lokale Cache auf dem PC und seine Bedeutung erklärt. Etwas Ähnliches findet sich in fast jedem größeren Netzwerk zusätzlich noch auf einem zentralen Rechner. Alle Internet-Anfragen (meist jedoch nur WWW) werden

über diesen Proxy-Server umgeleitet. Hier wird dann verglichen, ob die angeforderte Information nicht vielleicht kürzlich schon einmal angefordert wurde. Wenn das der Fall ist, wird sie nicht erst wieder aufwändig aus dem Internet heruntergeladen, sondern direkt vom Cache des Proxy-Servers an den PC des Benutzers übertragen – das geht wesentlich schneller und ist viel billiger. Nur bei noch nicht vorhandenen oder vielleicht inzwischen veralteten Informationen stellt der Proxy-Server die Verbindung ins Internet her, speichert die Informationen dann aber für eventuelle erneute Aufrufe wieder lokal ab.

In den Cache-Verzeichnissen eines Proxy-Servers finden Sie also ebenso bunte und aussagekräftige Informationen über die Internet-Nutzung im Unternehmensnetzwerk wie auf Ihrer lokalen Festplatte - nur eben von allen Benutzer(n)/-innen des Netzwerkes auf einem Haufen.

Auch viele spezielle Anwendungen, die der unternehmensinternen und –externen Kommunikation dienen, haben ähnlichen Charakter. So wird beispielsweise beim Einsatz des MS-Exchange-Servers oder von Lotus Domino – eines von beiden ist in fast jedem größeren Windows-Netzwerk zu finden - als zentrale Kommunikationsplattform jede ausgetauschte Information zentral verarbeitet. Somit wird jeder Termin, jeder Kontakt und jede Notiz, die Sie beispielsweise in MS-Outlook oder Lotus-Notes (die entsprechenden Client-Programme der genannten Server) eingeben, von den Servern zwischengespeichert. Dies geschieht beispielsweise, um Besprechungsanfragen zu synchronisieren, um Ihre Daten zu sichern oder um Ihnen das mobile Arbeiten an Notebooks bei gleichbleibendem Komfort zu ermöglichen.

Und jede Mail, die von Ihnen geschrieben wird, ist – zumindest kurzzeitig – auf dem Server im Klartext lesbar, nämlich mindestens so lange, bis sie weiterverschickt worden ist.

Zusammenfassend: In jedem Netzwerk gibt es - und muss es geben – einige zentrale Geräte, die schon aufgrund ihres Zwecks „mithören“. Die Frage ist, wie mit diesen Datensammlungen umgegangen wird.

Alle oben genannten Produkte – egal, ob es sich um Hardware oder Software handelt – protokollieren mehr oder weniger umfangreich mit. Und als Benutzer kann man sich dagegen nicht wehren, da die Protokolle in aller Regel zur Aufrechterhaltung des Betriebs benötigt werden und manchmal ihre Auswertung auch sinnvoll oder gar zwingend ist – beispielsweise nach einem Hackerangriff auf das Netz, nach einem Systemabsturz oder zum Auffinden von Schwächen oder Fehlern in der Infrastruktur.

## 12.4. Die Probleme:

- In vielen Fällen sind sich die Anwender/-innen nicht bewusst, dass solche Protokollierungen stattfinden und haben ein entsprechend unbedarftes Surf- und E-Mail-Verhalten.
- Als Anwender/-in kann man praktisch nicht herausfinden, was genau protokolliert wird und wie bzw. ob die Protokolle ausgewertet werden.
- Die ohnehin vorhandenen Datenbestände verleiten Vorgesetzte oder Administrator(en)/-innen leicht dazu, den/die Kolleg(en)/-innen „einen Blick über die Schulter zu werfen“ – sprich sie zu kontrollieren.

Diesen Problemen wird man mit technischen Mitteln nicht beikommen können, da sie systemimmanent sind. Man kann aber an der einen oder anderen Stelle zumindest versuchen, die Kontrolle zu erschweren, beispielsweise indem Mails verschlüsselt verschickt werden.

Aber die grundsätzliche Information, dass ein Anwender/-in A eine Mail an Anwender/-in B geschrieben hat, wann diese verschickt worden ist und wie groß sie war, ist nicht zu verschleiern.

---

**Diese Art der Überwachung kann nur durch organisatorische Maßnahmen unterbunden werden, beispielsweise durch Betriebsvereinbarungen, die festlegen, unter welchen Umständen Log-Protokolle geöffnet werden dürfen, wie lange sie gespeichert werden dürfen, und wer bei der Öffnung anwesend sein muss (Vier-Augen-Prinzip).**

---

Durch diese organisatorischen Regelungen wird eine eventuelle Überwachung zumindest eindeutig zu einer illegalen Handlung (sofern sie es nicht durch bestehende Gesetze ohnehin schon ist), schützt den Einzelnen aber nicht unbedingt vor Konsequenzen.

## 13. Servus Server! – Software für den Diener

Ähnlich wie die Key-Logger den lokalen PC bewusst überwachen, gibt es auch Software, die an den genannten zentralen Knotenpunkten lauscht.

- Das ist effektiver, da die Software nur an diesen Knotenpunkten installiert und administriert werden muss.
- Das ist besser, wenn man nicht möchte, dass die Anwender/-innen von der Überwachung erfahren. Denn der Einsatz solcher Spionage-Software kann „mit Bordmitteln“ praktisch nicht entdeckt werden.
- Das ist sicherer, da Benutzer/-innen und Benutzer im Normalfall keine Möglichkeit haben, an den Servereinstellungen etwas zu verändern – selbst wenn sie wissen, dass Überwachungsprogramme laufen (Key-Logger kann man durchaus deinstallieren, wenn man weiß, dass sie existieren und sich einigermaßen geschickt anstellt).

Die Funktionsweise solcher Software-Produkte unterscheidet sich stark. Oftmals binden sie sich direkt in eine der oben genannten Netzwerk-Komponenten ein oder stellen die Funktionalitäten gar selbst zur Verfügung (insbesondere, was Firewall- und Proxy-Funktionen betrifft).



Damit können sie – aus Sicht des/der Benutzer(s)/-in - fast in die Viren-Kategorie der „Trojanischen Pferde“ eingeordnet werden. Als „Trojanische Pferde“ werden Programme bezeichnet, die im Allgemeinen eine „Nutz-Funktion“ besitzen, also etwas, das der/die Anwender/-in gebrauchen kann und haben will, und eine „Schadens-Funktion“, die meist unbemerkt im Hintergrund andere Aktivitäten durchführt. Dazu gehören zum Beispiel Protokollierungen, der unbemerkte Versand von Informationen an Unberechtigte oder ganz einfach Funktionen, die den Rechner zerstören.

Alle Programme haben aber die gleiche Kernfunktion: den Netzwerk-Verkehr zu überwachen und „unberechtigte“ oder „anstößige“ Inhalte oder Aktivitäten in irgendeiner Weise zu melden oder den Zugriff zu verweigern.

### **13.1. Produktinformation**

Zwei Anbieter solcher „Spionage-Software“ sind die Firma SurfControl mit ihren Produkten „SuperScout Web Filter“ und „Super Scout E-Mail Filter“ und die Firma Websense mit ihrem gleichnamigen Produkt.

---

**SurfControl bietet mit „SuperScout Web Filter“ eher eine klassische Web-Filter-Lösung an:**

---

Das Programm wird am zentralen Übergabepunkt zum Internet installiert und überwacht dort jeden WWW-Zugriff. Dabei können von vornherein Regeln festgelegt werden, welche/-r Benutzer/-in was darf (bspw. kann ein Übertragungsvolumen für einzelne Benutzer/-innen festgelegt werden, es können zeitliche Beschränkungen vergeben werden etc.) und welche Internet-Adressen gefiltert werden sollen. Beim Aufrufen einer solchen gefilterten Adresse kann diese dann einfach abgefangen werden, so dass der/die Benutzer/-in nichts oder nur eine entsprechende Fehlermeldung sieht oder eine Alarm-Funktion ausgelöst wird. Die Auswertungsfunktionen von „SuperScout Web Filter“ sind vielfältig, da – je nach Einstellung – jeder Internet-Zugriff protokolliert und anschließend nach unterschiedlichen Kriterien ausgewertet werden kann: Beispielsweise nach dem Surf-Verhalten einzelner Personen oder wie oft eine bestimmte Seite im Internet aus dem Unternehmen heraus aufgerufen wurde oder nach ähnlichen Kriterien. Die „Access-List“ und „Deny-List“, also die Dateien, in denen festgelegt wird, welche Seiten als potenziell ungeeignet für die betrieblichen Aufgaben angesehen werden können, müssen dabei vom jeweiligen Unternehmen selbst erstellt werden.

Einen etwas anderen Weg geht die Firma Websense: In den Filter-Funktionen sind sich die beiden Programme recht ähnlich, aber die Pflege der „Deny- und Access-Listen“ kann hier zentral vorgenommen werden. Dazu beschäftigt Websense einen

ganzen Stab von Mitarbeiter/-innen, der bisher 2,3 Millionen Internet-Adressen bzw. 500 Millionen Internet-Seiten in rund 75 Kategorien aufgeteilt hat. Solche Kategorien sind beispielsweise „Online-Banking“, „Spiele“, „Lotto“, „Wirtschafts-News“ etc. Beim Einsatz von Websense kann dann jedem Mitarbeiter der Zugriff auf einzelne Kategorien verboten oder erlaubt werden – auch abhängig von unterschiedlichen Tageszeiten oder mit Zeit-Volumen oder nach anderen Kriterien.

Als besonderen Service bietet Websense ein „AfterWork-Portal“ an: Jede Internet-Seite, die ein/-e Mitarbeiter/-in in seiner/ihrer Arbeitszeit aufruft und die zu dieser Zeit für ihn/sie gesperrt ist, in der Freizeit aber zugänglich sein soll, kann in einer speziellen Liste erfasst werden. Dieses Portal kann der/die Mitarbeiter/-in dann nach getaner Arbeit „abarbeiten“.

Die Zugriffslisten werden zentral von der Firma Websense gepflegt (auf Wunsch mit kundenspezifischen Ausprägungen) und jede Nacht automatisch aktualisiert. Zusätzlich dazu können Unternehmen auch alle aufgerufenen Seiten, die nicht in den Websense-Katalogen vorhanden sind, automatisch an Websense zur zukünftigen Kategorisierung übermitteln.

Die Besonderheit daran ist: Die Kategorisierung wird ausschließlich von Menschen vorgenommen, die sich die Seiten betrachten und aufgrund des realen Inhalts beurteilen. Es gibt keine Stichwort-Suchen wie bei anderen Produkten, die dadurch zum Beispiel auch versehentlich „unkritische“ Seiten sperren könnten (und dieses in der Praxis auch tun).

---

**Websense wurde beispielsweise bei der Firma XEROX für die Überwachung von 92.000 Mitarbeitern und Mitarbeiter/-innen eingesetzt und auch die US-Army hat diese Software angeblich für 200.000 Arbeitsplätze lizenziert. Insgesamt gibt Websense die Anzahl der Lizenzen auf über 5 Millionen in über 8.400 Unternehmen an.**

---

Bemerkenswert ist auch der „SuperScout E-Mail-Filter“ von SurfControl. Dieser überwacht den gesamten E-Mail-Verkehr eines Unternehmens (sowohl eingehende als auch ausgehende Mails) auf unerlaubte Schlagworte und ähnliche Anzeichen für arbeitsfremde Tätigkeiten.

Dabei greift er sehr tief in die E-Mails ein: Im Gegensatz zu vielen anderen E-Mail-Filtern werden hier auch die E-Mail-Anhänge untersucht, bis hin zur automatischen Analyse von Bildern durch den „Virtual Image Agent“, der angeblich herausfindet, ob Bilder eventuell „nicht jugendfrei“ sind oder ähnliches. Auch blockt er (bspw. mit

PGP) verschlüsselte Emails ab, wenn diese von unberechtigten Personen innerhalb des Unternehmens verschickt wurden.

In der folgenden Tabelle sind einige der weiter verbreiteten Produkte genannt – zusammen mit einer Beschreibung, was sie genau machen und ob sie auch Nutz-Funktionen integrieren, die oftmals augenscheinlich ihren Einsatz rechtfertigen.

---

**SuperScout-Web-Filter**  
**SurfControl GmbH**  
**([www.surfcontrol.de](http://www.surfcontrol.de))**

---

- Filtert alle WWW-Zugriffe auf Basis von Schlagwort- Listen.
- Beschränkung der Zugriffe kann generell erfolgen oder beispielsweise nach Volumen (zeitlich oder kapazitativ) oder sonstigen Regeln.
- Erkennt auch den Inhalt von Bildern.
- Bietet detaillierte Auswertungsmöglichkeiten und Alarm-Funktionen an.
- Nutzwert: Benutzerabhängige Internet-Rechte können einfach festgelegt werden (zeitlich, volumenabhängig).

---

**SuperScout E-Mail-Filter**  
**SurfControl GmbH**  
**([www.surfcontrol.de](http://www.surfcontrol.de))**

---

- Filtert alle ein- und ausgehenden E-Mails auf Basis von Schlagwort-Listen.
- Auch E-Mail-Anhänge werden auf Schlagworte durchsucht.
- Erkennt auch den Inhalt von Bildern.
- Kann den Transport von verschlüsselten E-Mails verhindern.
- Alarm-Funktionen.
- Nutzfunktionen: Eingehende Mails werden ebenfalls kategorisiert und bspw. Werbung („Spam“) automatisch aussortiert. VirenScanner können einfach eingebunden werden.

---

**Websense Websense**  
**([www.websense.com](http://www.websense.com))**

---

- Filtert alle WWW-Zugriffe.

- Die zu filternden Internet-Seiten werden zentral von Websense gepflegt und von Menschen kategorisiert.
- Beschränkung der Zugriffe kann generell erfolgen oder beispielsweise nach Kategorien („Spiele“, „Online- Banking“ o.ä.), Volumen (zeitlich oder kapazitativ) oder sonstigen Regeln.
- Bietet detaillierte Auswertungsmöglichkeiten und Alarm-Funktionen an.
- Nutzfunktionen: Benutzerabhängige Internet-Rechte können einfach festgelegt werden (zeitlich, volumenabhängig).

Auch können unterschiedliche Einstellungen für „während der Arbeitszeit“ und „nach der Arbeit“ vorgenommen werden.

---

**Mail-Gear Symantec**  
([www.symantec.de](http://www.symantec.de))

---

- Filtert alle ein- und ausgehenden E-Mails auf Basis von Schlagwort-Listen.
- Auch E-Mail-Anhänge werden auf Schlagworte durchsucht, insbesondere auch komprimierte Dateien (ZIP), MS-Office-Dokumente und PDF-Dateien.
- Nutzfunktionen: Eingehende Mails werden ebenfalls kategorisiert und bspw. Werbung („Spam“) automatisch aussortiert.

---

**Internet-Manager Elron**  
([www.elronsw.de](http://www.elronsw.de))

---

- Besteht aus mehreren Modulen für das Filtern von WWW-Zugriffen und E-Mails auf Basis von Schlagwort- Listen.
- Bietet detaillierte Auswertungsmöglichkeiten.
- Nutzwert: Benutzerabhängige Internet-Rechte können einfach festgelegt werden (zeitlich, volumenabhängig).

Eingehende Mails werden ebenfalls kategorisiert und bspw. Werbung („Spam“) automatisch aussortiert.

---

**WebSpy ProtectCom**  
([www.protectcom.de](http://www.protectcom.de))

---

- Filtert alle Internet-Zugriffe (auch andere Dienste als WWW wie bspw. FTP, Instant-Messaging, Chat) auf Basis von Schlagwort-Listen.

- Ermöglicht die Festlegung von Internet-Richtlinien.
- Umfangreiche Protokollierungs- und Alarm- Funktionen (Module „Sentinel“ und „Analyzer“).
- Datenbankgestützte (und damit effektive) Protokollierung und Auswertung.

**Internet-Watcher 2000 Bernard D&G**  
 ([www.internetwatcher.de](http://www.internetwatcher.de))

- Filtert alle WWW-Zugriffe auf Basis von Schlagwort- Listen, überwiegend für den privaten Einsatz entwickelt.
- Beschränkung der Zugriffe kann „On the Fly“ erfolgen, d.h. es können Internet-Seiten, auf denen bestimmte Schlagworte stehen, automatisch per Passwort geschützt werden.
- Bietet detaillierte Auswertungsmöglichkeiten.
- Nutzwert: Ist gleichzeitig ein Internet-Proxy zum Zugriff mehrerer Rechner auf einen Internet- Anschluss. Enthält weitere Funktionen wie Werbeflocker zur Beschleunigung des Seitenaufbaus und Cookie-Filter.

Aber auch viele Programme, die eigentlich von ihrer Kernfunktion her andere Aufgaben haben, enthalten solche Kontrollfunktionen „nebenbei“. Beispielsweise Symantec Web Security:

Dieses Programm ist eigentlich ein (leistungsstarker) Internet-Viren-Scanner für FTP und WWW, der aber gleichzeitig auch nach Schlüsselworten sucht und ähnlich den oben genannten Programmen verfährt.

## 13.2. ...UND WIE MAN SICH DAGEGEN WEHRT

Wie eingangs bereits gesagt: Normale Benutzer/-innen und Benutzer können sich gegen solche Programme mit technischen Mitteln fast gar nicht wehren!

Sie können nur versuchen herauszubekommen, ob Sie überhaupt überwacht werden und können den Überwachern das Leben ein wenig schwerer machen. Leider funktionieren viele der folgenden Tipps nur dann, wenn die PCs und das gesamte Netzwerk einigermaßen großzügig aufgebaut sind.

**Konkret heißt das:**  
**Wenn Ihr Unternehmen Ihnen verbietet**

- Software überhaupt auf den Rechner zu kopieren (beispielsweise durch gesperrte Disketten- und CD-Rom-Laufwerke, Download-Verbote aus dem Internet und automatisch entfernte E-Mail-Anhänge),
- Software zu installieren oder sogar nicht von dem/der Systemadministrator/-in „freigegebene“ Software auszuführen,
- die Einstellungen in Anwendungen (insbesondere in Browsern und E-Mail- Programmen) zu verändern oder gar nur einzusehen, dann haben Sie ohne eine echte „Hacker-Mentalität“, die sie letztendlich aber den Arbeitsplatz kosten kann, keine Chance, irgendetwas an der Situation zu verändern.

## 14. Spionage-Hardware

Zur Überwachung von Computerarbeitsplätzen wurde auch spezielle Hardware entwickelt, die z.B. Ihre Tastatur überprüft und jeden Tastenanschlag protokolliert. So können alle Ihre Aktivitäten an Ihrem Rechner nachvollzogen werden.

---

### Tastaturstecker

---

Ein Tastaturstecker ist ein kleines Gerät, das zwischen Tastatur und Computer angeschlossen wird - ähnlich einem Adapter. Das Gerät zeichnet alle Tastaturaktivitäten auf und kann zu einem späteren Zeitpunkt ausgelesen werden.

Einen derartigen Hardware-Eingriff können Sie selber prüfen: Verfolgen Sie das Tastaturkabel und sehen Sie nach, ob sich ein ungewöhnliches Gerät daran befindet. Das ist noch nicht alles! Es gibt noch weitere Möglichkeiten der Datenüberwachung, auf die wir Sie hier aufmerksam machen möchten:

Wie bereits erwähnt können natürlich auch zentrale Geräte, wie z.B. Firewalls oder Server, zum „Mithören“ benutzt werden. Diese Geräte protokollieren die Vorgänge aller Firmenrechner zur Aufrechterhaltung des Betriebs. Werden die Protokolle bei Problemen sinnvoll ausgewertet, können eventuelle Fehler behoben werden. Ihre Software kann aber auch zur Überwachung der Beschäftigten genutzt werden. Ferner gibt es spezielle Software an zentralen Knotenpunkten des Netzwerkverkehrs. Diese Software meldet sofort unberechtigte Inhalte oder Aktivitäten an den Sysadmin weiter. Dieser kann schon durch Voreinstellungen bestimmte Inhalte verbieten oder gegebenenfalls direkt in Ihre Anwendungen eingreifen. In beiden Fällen besteht für Sie keine Möglichkeit den Servereinstellungen mit technischen Mitteln beizukommen, da diese Programme systemimmanent sind.

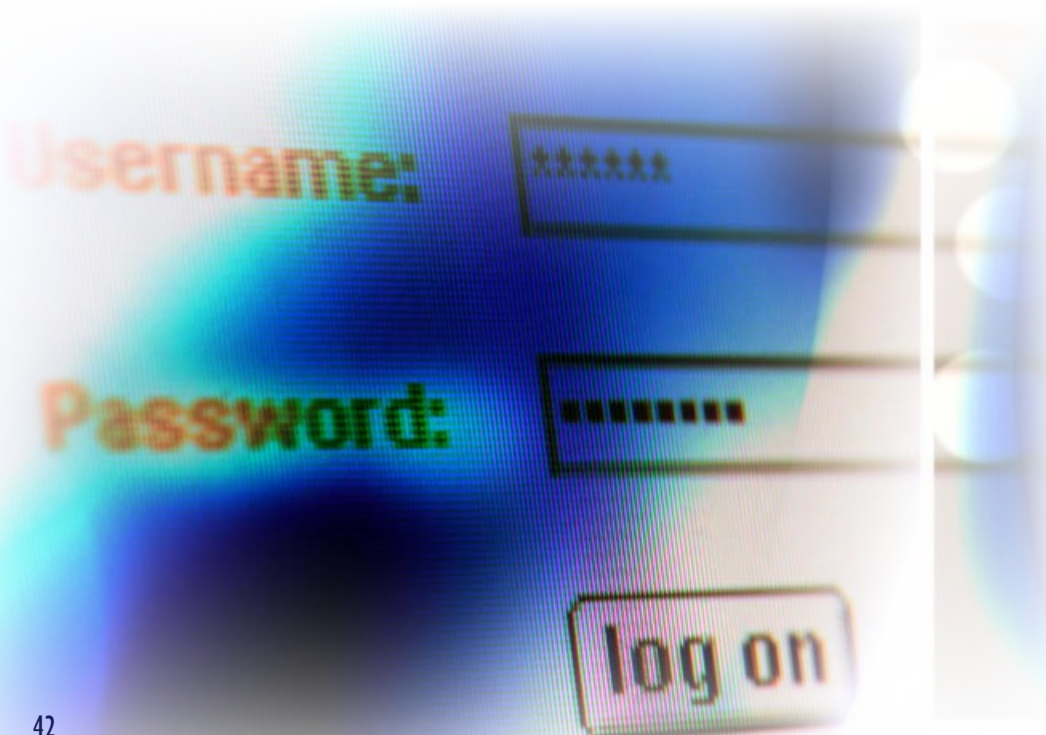
# 15. Wie gut ist Ihr Passwort?

Mit Passwörtern kann man den Zugang zu Daten manchmal erschweren. So können Sie mit Ihrem Passwort den Zugang zu Ihrem Computer vor Kolleg(en)/-innen schützen – aber nicht vor den Administrator(en)/-innen.

## 15.1. Passwortqualität

### Aber wie gut ist Ihr Passwort?

Passwörter sind nur dann gut, wenn sie geheim bleiben, nicht zu erraten und möglichst abstrakt sind. In der Praxis werden oft sehr schlechte Passwörter verwendet und diese auch noch schlecht versteckt. Sie sind oft durch das sogenannte „Social Engineering“ leicht herauszufinden. So hatte einer der größten Telekom-Provider Österreichs einer IT-Security-Firma den Auftrag gegeben ihr System zu hacken, um auf diese Art und Weise die IT-Sicherheit der Firma zu überprüfen. Nach weniger als einer Stunde war es geschafft. Beschäftigte hatten ihre Passwörter unter Mouse-Pads, Bildschirmen etc. notiert.



Kennwörter sind nur dann gut, wenn sie nicht leicht zu erraten sind und auch gegen technische Angriffe einigermaßen sicher sind – zum Beispiel gegen sogenannte Brute-Force-Attacken. Das sind Angriffe mit brutaler Gewalt, nämlich durch einfaches Ausprobieren aller Kombinationsmöglichkeiten. Es wird angenommen, dass bis zu 5.000.000 Kombinationen pro Minute ausprobiert werden können. Diese Zahl wird beispielsweise von Passwortknackern für MS-Word erreicht.

### **Leicht assoziierbare Passwörter:**

- Namen von Angehörigen oder Haustieren
- Autokennzeichen oder Marken
- Geburtsdaten
- Intuitive Passwörter
- Monatsnamen
- Jahreszeit-Ereignisse (Feiertage etc.)
- Standard-Wörter wie „Geheim“, „Kennwort“ oder eine Wiederholung des eigenen Anmelde-Namens
- Sichtbare Passwörter
- Bezeichnung des Computers/Monitors/Telephons auf dem Schreibtisch
- Maler eines Bildes, das im Raum hängt

Oft findet sich das Passwort als kleiner Zettel unter der Tastatur oder dem Telefon, in der Schreibtisch-Schublade, oder aber ganz offensichtlich als „unscheinbares Wort“ irgendwo auf dem Schreibtisch oder der Pinwand.

## **15.2. Testen Sie Ihr Passwort**

Dieser Test untersucht Ihr Kennwort auf seine Sicherheit gegen solche Angriffe und sagt Ihnen, wie lange es in etwa dauert, das Kennwort auf diesem Weg herauszubekommen

<https://ssl.kundenserver.de/root.customite.de/kunden/spionage/passqual.php3>

.....  
**Nach dem Test Ihres Passwortes sollten Sie es ändern, denn auch dies ist nachvollziehbar!**  
.....

## **15.3. Wie macht man gute Passwörter?**

Intuitive, leicht assoziative und sichtbare Kennwörter sind schlecht. Außerdem sollte von „echten“ Worten einer Sprache unbedingt Abstand genommen werden.

Die absolute Mindestanforderung an ein Passwort sollte 7 Stellen, gemischt aus Buchstaben und Zahlen sein. Dann dauert die Suche danach schon ein paar Tage. Wenn zusätzlich Sonderzeichen (Satzzeichen o.ä.) verwendet werden, ist man auf der sicheren Seite. Bei Systemen, die nur sechstellig Passwörter zulassen, sind Sonderzeichen Pflicht! Ansonsten ist das Kennwort nach spätestens 8 Stunden geknackt.

### **Eine Möglichkeit, ein gutes Passwort zu bilden, ist beispielsweise folgende:**

Man nimmt einen kurzen, prägnanten Satz, etwa ein Zitat, das man sich leicht merken kann. Beispielsweise aus Goethes „Faust“ den Satz „Zwei Herzen schlagen ach in meiner Brust!“. Dann nimmt man von jedem Wort nur den Anfangsbuchstaben und das Satzzeichen: „zhsaimb!“.

Das ist schon ein ziemlich perfektes Kennwort. Um ganz sicher zu gehen, oder wenn man das Kennwort regelmäßig ändern muss, kann man auch noch Zahlen einbinden, beispielsweise den Monat (01 für Januar, 02 für Februar usw.): „zhsaimb!03“. So lange die Kombination nicht zu durchschaubar ist und vor allem das genaue System niemandem verraten wird, ist dieses Kennwort perfekt! Es über Kombinationsversuche herauszubekommen würde auch unter besten Bedingungen viele Jahre dauern. Wem literarische Zitate nicht liegen, der kann natürlich auch Teile des Lieblingsliedes, den Titel des gerade gelesenen Buches oder andere „bewegende“ und leicht zu merkende Sätze verwenden.

## **15.4. Passwortschutz von Word-Dateien**

Öffnen Sie die zu schützende Word-Datei. Gehen Sie dann in der oberen Menüleiste unter dem Feld „Extras“ auf „Optionen“. Unter der Registrierkarte „Speichern“ finden Sie ganz unten „Optionen für gemeinsamen Zugriff“. Dort können Sie nun ein Passwort für Ihre Datei eingeben.

## **16. Verschlüsse Dich**

### **16.1. Der einfachste Weg: E-Mail-Verschlüsselung**

Schon seit vielen Jahren ist das Thema E-Mail-Verschlüsselung in aller Munde. Um so erstaunlicher, dass sie im Alltag kaum oder zumindest nicht großflächig eingesetzt wird. Das wohl am häufigsten genannte Produkt beim Thema Verschlüsselung ist das Programm „Pretty Good Privacy“ (PGP). PGP ist ein seit vielen Jahren in der Standard-Ausführung kostenlos erhältliches und eigentlich auch relativ weit verbreitetes Programm zur E-Mail-Verschlüsselung. Dabei gilt der verwendete Verschlüsselungsalgorithmus aus heutiger Sicht als „sicher“, also nicht zu knacken.

PGP ist ein von Network Associates Inc. vertriebenes Programm, das sowohl über kryptographische Verschlüsselungsfunktionalitäten verfügt, als auch zur digitalen Signatur von Dateien und E-Mails geeignet ist. PGP verwendet hierzu ein Public Key Verfahren und Zertifikate, die im Gegensatz zu den meisten Verfahren grundsätzlich ohne Trustcenter auskommt. PGP basiert auf dem „Web of Trust“, bei dem der öffentliche Schlüssel unter Bekannten ausgetauscht und gegenseitig als vertrauenswürdig zertifiziert wird. Der Verzicht auf ein zentrales Trustcenter führte zu einer schnellen Verbreitung von PGP-Schlüsseln.

Der Haken: Um PGP verwenden zu können, muss man relativ viel über die Theorie der Verschlüsselung wissen, das Public- und Private-Key-Verfahren kennen und verstanden haben, und dann auch noch für die Installation einigen Forscherdrang mitbringen. Alles Faktoren, die beim „normalen“ User nicht gegeben sind, oder für die – wie so oft – keine Zeit zum Erlernen zur Verfügung steht.

Dabei ist das Verfahren eigentlich ganz einfach: Wenn man jemandem eine mit PGP verschlüsselte E-Mail schicken möchte, so muss man dessen öffentlichen Schlüssel (Public-Key) – eine etwas komplizierte Zeichenkombination aus Buchstaben und



Zahlen - kennen. Das ist nicht weiter schwer. Dieser Schlüssel findet sich bei Firmen oftmals auf der Internet-Seite oder man fragt die entsprechende Person einfach direkt. Die E-Mail wird dann mit diesem öffentlichen Schlüssel verschlüsselt und verschickt. Ab dann kann niemand mehr den Inhalt lesen - nur der/die berechnete Empfänger/-in, der/die den passenden privaten Schlüssel („Private-Key“) dazu hat, kann den Inhalt wieder lesbar machen.

---

**Allerdings gibt es in der Praxis jede Menge Schwierigkeiten:**

---

- Das „Key-Management“ ist leider nicht ganz einfach. Die ursprünglich sehr gute Idee, den öffentlichen Schlüssel noch „Vertrauenszertifikate“ mitzugeben (also zu hinterlegen, ob und welche Benutzer diesem öffentlichen Schlüssel vertrauen, denn theoretisch ist es natürlich auch möglich, dass man einen Text mit einem „falschen“ öffentlichen Schlüssel verschlüsselt, dessen privates Gegenstück in den Händen von Benutzern mit böswilligen Absichten ist), verwirrt „Kryptographie-Anfänger“ nur.
- Man sollte sich sicher sein, dass der öffentliche Schlüssel des/der Empfänger(s)/-in noch aktuell ist, der/die Empfänger/-in das private Gegenstück also tatsächlich auch noch hat. Zumindest bei Privatanwendern ist es oft der Fall, dass – wenn PGP nicht regelmäßig verwendet wird - erzeugte Schlüssel schnell in Vergessenheit geraten.
- Der/die Empfänger/-in muss selbst natürlich das gleiche Verschlüsselungsverfahren – im Beispiel PGP - installiert haben, um die Mail überhaupt lesen zu können. Das ist wohl der Hauptgrund, warum E-Mails nur sehr selten verschlüsselt werden, denn gerade bei geschäftlicher Korrespondenz weiß man das im Allgemeinen nicht.
- Außerdem sollten dann natürlich die öffentlichen Schlüssel der möglichen Empfänger/-innen auch wieder irgendwo aufgehoben werden – doch viele Firmen tun sich schon mit einer normalen Adressverwaltung schwer.
- Die Einbindung in viele E-Mail-Programme ist leider nicht ganz glücklich gelöst, und anstatt Automatismen einzubauen, die beispielsweise bei jedem Versand automatisch nachfragen, ob der Text verschlüsselt übertragen werden soll, sind derzeit immer noch explizite manuelle Tätigkeiten des/der Benutzer(s)/-in vor dem Versand notwendig – die nur allzu oft vergessen werden, selbst wenn alle anderen Bedingungen erfüllt sind.

Diese Hürden halten viele Unternehmen auch davon ab, „standardmäßig“ PGP zu verwenden, auch wenn es auch und gerade für den normalen geschäftlichen E-Mail-Verkehr sehr sinnvoll wäre. Denn oftmals würde sich die eine oder andere

Unternehmensleitung die Haare raufen, wenn sie wüsste und verstehen würde, dass die meisten verschickten E-Mails mit potenziell unternehmenskritischen Informationen wie Vertragsverhandlungen oder Notizen zu Akquisegesprächen im Klartext und für jeden (laienhaften) Lauscher lesbar sind.

Trotz aller Vorteile von PGP und der eigentlich existierenden zwingenden Notwendigkeit, solche Verschlüsselungen prinzipiell einzusetzen, hat sich das System noch nicht großflächig durchgesetzt und wird es wohl auch in den nächsten Jahren nicht tun.

Wenn Sie aber ein wenig Erfahrung mit Computern haben, den nötigen „Forscherdrang“ mitbringen, die notwendigen Berechtigungen haben, um PGP auf Ihrem Arbeitsplatz zu installieren, und dann auch noch Ihren „Gegenüber“ von dieser Notwendigkeit überzeugen können (und natürlich auch er oder sie die entsprechenden Voraussetzungen mitbringt), ist PGP eine gute und sichere Wahl, Lauscher auszusperrern und die Privatsphäre zu wahren. Allerdings gibt es – wie oben erwähnt – inzwischen auch E-Mail-Filter-Programme, die solche verschlüsselten Mails erst gar nicht aus dem Unternehmen herauslassen.

---

**PGP selbst sowie die entsprechenden Dokumentationen können Sie unter <http://www.pgpl.org/> kostenlos downloaden.**

---

## **16.2. Tierliebe: work@IT liebt aber GnuS**

GnuPG (GnuPrivacyGuardist) ist ein vollständiger und freier Ersatz für PGP. Es benutzt den patentierten IDEA Algorithmus nicht und kann deswegen ohne Einschränkungen benutzt werden. GnuPG ist eine RFC 2440 (OpenPGP) kompatible Anwendung.

---

**Die Version 1.0.0 wurde am 7. September 1999 freigegeben. Die aktuelle stabile Version ist 1.2.6.**

---

GnuPG ist Freie Software. Unter den Bedingungen der GNU General Public License kann es frei benutzt, geändert und weitergegeben werden!

Klassische Methoden zur Verschlüsselung benutzen nur einen Schlüssel. Der/die Sender/-in verschlüsselt seine/ihre Nachricht mit diesem Schlüssel, und der/die Empfänger/-in entschlüsselt ihn mit demselben wieder. Damit das funktioniert, muss der/die Empfänger/-in vorher den Schlüssel bekommen haben, und zwar auf einem sicheren Kommunikationskanal, da sonst Unbefugte in Kenntnis des Schlüssels

gelangen könnten. Also braucht man einen sicheren Kommunikationskanal, aber wenn man den hat, braucht man auch nicht mehr zu verschlüsseln.

Public Key Verfahren (auch: asymmetrischen Verfahren) beseitigen dieses Problem, indem zwei Schlüssel erzeugt werden: Der öffentliche, der über beliebige Kommunikationskanäle verschickt werden kann und der private, den nur der/die Besitzer/-in kennt. Idealerweise ist der private Schlüssel nicht mit dem öffentlichen rekonstruierbar. Der/die SenderIn verschlüsselt die Nachricht mit dem öffentlichen Schlüssel des/der Empfänger(s)/-in. Entschlüsselt wird die Nachricht dann mit dem privaten Schlüssel des/der Empfänger(s)/-in. Nach diesem Schema kann man demnach effektiv verschlüsseln, ohne über einen sicheren Kommunikationskanal zu verfügen.

Ein ganz wichtiger Punkt ist aber die Geheimhaltung des privaten Schlüssels. Er darf auf keinen Fall in fremde Hände geraten, auch nicht über das Netz verbreitet werden. GnuPG via telnet zu benutzen, ist zum Beispiel eine ziemlich schlechte Idee. (Eigentlich sollte man telnet sowieso durch ssh ersetzen)

---

**Genauere Informationen zu GnuPG und der GNU General Public License finden Sie unter <http://www.gnu.org> oder <http://www.gnupg.org>**

---

## **16.3. So oft wie möglich verschlüsselte Seiten verwenden**

Neben dem für WWW üblichen HTTP („Hyper-Text-Transfer-Protokoll), über das die gesamte Kommunikation zwischen dem Browser und dem Internet-Server abgewickelt wird, gibt es noch ein zweites Protokoll für WWW, das eine verschlüsselte Datenübertragung verwendet.

Es handelt sich dabei um HTTPS („Hyper-Text-Transfer-Protokoll-Secure“). Manche Internet-Seiten, insbesondere solche, welche die Eingabe von persönlichen Informationen wie Kreditkartennummern o.ä. verlangen, bieten daher oft zusätzlich zur „normalen Seite“ auch eine HTTPS-Version an. Auf diesen können Sie relativ unbehelligt surfen. In eventuellen Protokollen ist zwar zu erkennen, welche Seiten Sie aufgerufen haben, nicht aber, was Sie dort gemacht haben, also welche Informationen Sie dort gelesen oder hingeschickt haben.

Diese Möglichkeit bietet sich also beispielsweise bei der Diskussion in Internet-Foren an, wo Sie eventuell Informationen eintragen, die nicht unbedingt für den Arbeitgeber bestimmt sind.

**Das einzige Problem:** Sie haben keinen Einfluss darauf, welche Seiten mit diesem sicheren Protokoll angeboten werden, da dieses serverseitig eingerichtet werden

muss und die meisten Anbieter von Diskussionsforen und ähnlichen Diensten derzeit leider (noch) keine entsprechenden HTTPS-Versionen haben.

Wann immer aber diese Funktion zur Verfügung steht, sollten Sie sie nutzen! Sie erkennen diese oft an dem Schlagwort „SSL“, an dem „https:“ in der Adressleiste oder an einem Schlüsselsymbol im Browser.

## **16.4. Dienste maskieren und Ziele verbergen**

### **Einen etwas anderen Weg geht ein Programm namens HTTPPort 3:**

Hier geht es weniger darum, Spuren direkt zu verwischen, als vielmehr darum, sie erst gar nicht entstehen zu lassen und Internet-Techniken zu nutzen, die ansonsten im Netzwerk verboten sind – aus welchen Gründen auch immer. Beispielsweise springen viele Firewalls samt ihrer Überwachungsfunktionen erst dann an, wenn „unberechtigte Dienste“ aus dem Netzwerk aufgerufen werden.

HTTPPort 3 liefert aber – mit ein wenig Aufwand – auch die Möglichkeit, alle Internet- Aktivitäten vollständig zu verheimlichen. Um das Verfahren zu verstehen, muss ein klein wenig tiefer auf das im Internet übliche TCP/IP-Protokoll eingegangen werden:

Jeder Rechner im Internet hat (mindestens) eine eindeutige IP-Adresse, also praktisch einen eindeutigen Namen. Da es aber mehrere unterschiedliche Arten von Internet-Diensten gibt – beispielsweise HTTP, HTTPS, FTP (File-Transfer-Protokoll zum Übertragen von Dateien), POP-Mail (Post-Office-Protocoll zum Abrufen von E-Mails), SMTP (Simple-Mail-Transfer-Protokoll zum Verschicken von E-Mails) und viele weitere mehr – reicht die IP-Adresse alleine nicht aus um festzulegen, was mit einem Datenpaket passieren und von welchem Programm es also verarbeitet werden soll. Daher wird zusätzlich zur IP-Adresse noch eine sogenannte Port-Nummer mit übertragen, die den entsprechenden Dienst bestimmt. Jedem Dienst ist dabei (mindestens) eine Nummer zugeordnet. HTTP hat beispielsweise standardmäßig den Port 80 und FTP den Port 21.

Viele Firewalls sind so konfiguriert, dass sie Port-80-Anfragen (HTTP) und oftmals auch Port-443-Anfragen (HTTPS) ohne Probleme durchlassen und aufgrund der Flut an Zugriffen entsprechende Protokolle gar nicht ausgewertet werden. Ganz anders verhält es sich jedoch mit anderen Diensten wie beispielsweise den beliebten Instant-Messenger-Systemen oder dem Internet-Relay-Chats (IRC). Diese senden auf anderen Ports und werden oftmals von der Firewall blockiert. Oder aber – noch schlimmer – es springen entsprechende Protokollierungs- oder Alarmfunktionen an, die das „verdächtige“ Treiben beobachten sollen.

Für dieses Problem wurde das Programm HTTPPort 3 entwickelt ([www.htthost.com](http://www.htthost.com)), das es möglich macht, „unzulässige“ Dienste so umzulenken, dass sie von der Firewall durchgelassen werden und ihre „wahre Identität“ erst außerhalb des Firmennetzes zu erkennen geben. Es gibt dabei zwei unterschiedliche Modi:

Im ersten Modus kann man HTTPPort 3 so konfigurieren, dass die „wahre Identität“ direkt beim Verlassen des Firmennetzes preisgegeben wird. Das funktioniert durch einen Trick (keinen Fehler!) im HTTPS-Protokoll. Dort kann man nämlich explizit einen „Ziel-Port“ angeben, mit dem kommuniziert werden soll.

Innerhalb des Firmennetzwerks wird somit immer der „unverdächtige“ HTTPS-Port 443 angesprochen, dieser wird jedoch beim Verlassen automatisch auf den gewünschten Port „umgeroutet“. Somit ist es also möglich, beliebige Internet-Dienste in Anspruch zu nehmen, ohne besonders aufzufallen.

Aber Achtung: Damit das funktioniert, kann trotz der Verwendung des eigentlich „sicheren“ HTTPS-Ports keine Verschlüsselung verwendet werden, die von Ihnen übertragenen Daten sind also in entsprechenden HTTPS-Protokollierungen im Klartext zu lesen!

**Der zweite Modus ist aufwändiger einzurichten, liefert aber dafür die Möglichkeit des absolut anonymen Surfens aus Unternehmensnetzwerken heraus!**

Passend zum HTTPPort-3-Client (dem Programm, das auf Ihrem Rechner läuft und das Vertauschen der Ports vornimmt) gibt es auch noch ein entsprechendes Server-Programm namens HTTHost. Dessen Verwendung wird bei manchen Server-Betreibern als besonderer Service meist kostenlos oder zumindest kostengünstig ermöglicht, man kann es aber mit ein wenig Geschick und beispielsweise einer privat vorhandenen Flatrate am heimischen PC auch selber einrichten.

Jede Internet-Anforderung (auch die aus einem normalen Browser heraus) wird von Ihrem Client „bearbeitet“, die eigentliche Zieladresse sowie eventuell vorhandene weitere Informationen verschlüsselt und ausschließlich an den HTTPPort-3-Server geschickt (im besten Fall Ihren eigenen privaten Rechner). Dieser Server entschlüsselt die Daten wieder und leitet Ihre ursprüngliche Anfrage ganz normal weiter.

Mehr dazu finden Sie auf den Seiten von HTTPPort unter [www.htthost.com](http://www.htthost.com) im Bereich „HTTPPort /FAQ“

Das Einzige, was eventuell vorhandenen Lauschern bei diesem Verfahren also auffällt, ist, dass Sie immer nur den gleichen Zielrechner ansprechen, egal was Sie machen (zugegeben, auch ein wenig auffällig, aber zumindest kein Grund für einen direkten Verdacht). Außerdem wird diese Tatsache im Regelfall nicht bemerkt werden, da der Zielrechner in den entsprechenden Überwachungsprogrammen

nicht als „potenziell verdächtig“ eingetragen sein dürfte und somit normale Alarm-Funktionen versagen. Nur wenn man ganz explizit alle Ihre Aktivitäten überwacht, fällt überhaupt etwas auf. HTTPPort 3 ist also eine gute Möglichkeit, unerkannt aus Firmennetzen heraus im Internet zu surfen. Die Einschränkungen sind „nur“: Sie müssen auf Ihrem Arbeitsplatz-PC das Recht haben, Programme zu installieren, Sie müssen die Einstellungen Ihres Internet-Browsers verändern dürfen und Sie müssen einen öffentlich zugänglichen HTTPPort 3-Server finden oder ihn selber auf dem heimischen PC (oder dem eines Freundes) installieren. Außerdem ist nichts über die Stärke der Verschlüsselung bekannt, ob sie also wirklich so sicher ist, dass sie nicht mit vertretbarem Aufwand geknackt werden kann. Internet-Aufrufe verschlüsseln

**Ein weiteres interessantes Projekt um die Anonymität im Internet auch vom Arbeitsplatz aus zu wahren, befindet sich gerade an der Technischen Universität Dresden in der Entwicklung.**

Der Name lautet „**JAP, Anonymity is not a crime**“. Es ist von der Grundidee der verschlüsselten Datenübertragung durch das Unternehmens-Gateway dem Programm HTTPPort 3 ganz ähnlich, bezieht sich allerdings nur auf WWW-Zugriffe, die direkt über Port80 übertragen werden. Dafür hat es jedoch den Vorteil, dass die Anonymisierung nicht bei dem Rechner mit dem Server-Programm endet (denn dort wird die ursprüngliche Information ja wieder in Klartext umgewandelt), sondern auch innerhalb der Kommunikation im Internet gilt. Der Trick dabei ist, dass alle Internet-Anfragen auf Ihrem Rechner mehrfach verschlüsselt werden und diese verschlüsselten Datenpakete zu einem „Anon-Server“ übertragen werden (ähnlich der oben dargestellten HTTPHost-Methode). Von dort aber werden die Datenpakete verschlüsselt auf unterschiedliche Proxy-Server verteilt („Mix-Kaskade“), wobei jeder nur einen Teil des Datenpaketes entschlüsselt. Damit kennt jeder dieser Proxys nur einen Teil der Informationen (beispielsweise welche IP-Adresse die Anfrage abgesendet hat oder(!) welche Anfrage gesendet wurde, nicht aber beides gleichzeitig), und das Surfen funktioniert wirklich anonym.

**Der Haken:** Auch JAP funktioniert nur, wenn Sie die Einstellungen in Ihrem Webbrowser ändern und Programme installieren dürfen, und das ist an Arbeitsplatz- Rechnern oftmals nicht der Fall. Außerdem befindet sich JAP derzeit noch in der Entwicklung und ist erst in wenigen Teilen realisiert.

Ein gelegentlicher Blick auf die Website des Forschungsprojektes unter <http://anon.inf.tu-dresden.de> dürfte sich jedoch lohnen, und derzeit ist die JAPForschungsgruppe über „Test-Benutzer“ sehr erfreut.

Allerdings muss man hier ein wenig Pioniergeist mitbringen.

# 17. Mission accomplished

---

## **DIE Methode zur anonymen Internet-Nutzung gibt es nicht!**

---

Kryptographie – also die Verschlüsselung - ist eine Möglichkeit, wenigstens einzelne Aktivitäten zu „verstecken“. Aber spätestens, wenn Sie im Unternehmensnetzwerk nicht das Recht haben, Programme zu installieren und/oder die Einstellungen der Internet- Programme zu ändern, gibt es keine Möglichkeit, die Spuren zu verwischen. Sie können nur versuchen, einige der beschriebenen Tricks anzuwenden, um es potenziellen Spionen wenigstens ein bisschen schwerer zu machen und ansonsten nur auf der Hut sein.

Auch wenn Sie keine der von uns beschriebenen Anzeichen für eine Überwachung an Ihrem Arbeitsplatz finden, kann es dennoch möglich sein, dass Sie von Ihrem Chef kontrolliert werden. Daher sollten Sie das Thema Arbeitsplatzüberwachung offen gegenüber Ihrem Betriebsrat ansprechen oder sich an die IG work@IT wenden:  
<http://www.interesse.at/it>

---

**Bitte führen Sie KEINE unserer Anleitungen aus  
ohne vorher Ihre Rechte mit dem Betriebsrat  
Ihres Unternehmens abgeklärt zu haben!**

---

Impressum:

Herausgeber, Verleger und für den Inhalt verantwortlich:

Interessengemeinschaft work@IT - Die GPA-Initiative für Menschen in IT-Berufen

Börsegasse 18, A-1013 Wien

Fotos: Brand X Pictures

# Don't panic. Join us:



<http://www.interesse.at/join/index.htm>

Mit freundlicher Unterstützung von verdi-innotec.

