

# Der Chef surft mit

Technische Möglichkeiten der Mitarbeiterinnen- und  
Mitarbeiter-Kontrolle bei der Internet- und E-Mail Nutzung  
und wie man sich davor schützen kann

- teilweise überarbeitet im November 2008 -

---

Einleitung .....	2
Die technischen Grundlagen .....	4
Die Überwachung am PC .....	5
Gegen Gelegenheits-Lauscher kann man sich wehren .....	5
Setz dich und nimm dir 'nen Keks .....	5
Cache as Cache can .....	7
Spion wider Willen .....	7
Schuldig! .....	8
Tastensammler .....	8
... und wie man sich dagegen wehrt .....	11
Die zentrale Überwachung .....	13
Kein Kraut gewachsen .....	14
Der Spion im Server .....	15
... und wie man sich dagegen wehrt .....	17
Fazit .....	23

## Einleitung

Um es vorweg zu nehmen: Als Mitarbeiterin und Mitarbeiter in einem restriktiv aufgebauten Unternehmensnetzwerk hat man mit technischen Mitteln praktisch keine Möglichkeiten, sich vor all zu neugierigen Vorgesetzten zu schützen. Nur eine bewusste und verantwortungsvolle Nutzung der elektronischen Kommunikationsmöglichkeiten durch die Mitarbeiter und Mitarbeiterinnen und organisatorische Regelungen durch die betriebliche Interessenvertretung können der totalen Überwachung einen Riegel vorschieben oder sie zumindest in die Illegalität drängen. Eine gesunde Paranoia kann also bei der Internet- und E-Mail-Nutzung aus Unternehmensnetzwerken heraus nicht schaden.

Gründe, Mitarbeiterinnen und Mitarbeiter bei ihren Online-Aktivitäten zu überwachen, gibt es augenscheinlich mehr als genug:

- Es geht um das Entdecken von verschwendeten Zeitressourcen durch privates Surfen, E-Mails oder Spielen am Arbeitsplatz-PC. Wohl dem wichtigsten Grund, der - wenn man den Statistiken Glauben schenken darf - auch tatsächlich die Effektivität in Unternehmen merklich beeinträchtigt und Produktivitätsausfälle in Millionenhöhe beschert. Auch wenn die „paar Minuten“ bei eBay, Wer-Kennt-Wen oder Google Earth jedem einzelnen vernachlässigbar erscheinen, haben Sie schon im Jahr 2000 - als insbesondere viele der zeitfressenden Community-Portale noch gar nicht existierten - schon einen Produktionsausfall in Höhe von umgerechnet 26 Milliarden Euro generiert<sup>1</sup>.
- Es geht um den Schutz der sehr hohen Investitionen in die unternehmensinterne Netzinfrastruktur, die durch allzu eifriges surfen oft genug an ihre Kapazitätsgrenzen stößt.
- Es geht um das Aufdecken von kriminellen Machenschaften am Arbeitsplatz. So kann ein Großkonzern einen beträchtlichen Image-Schaden erleiden, wenn seine Mitarbeiterinnen und Mitarbeiter über die internen Netzwerke beispielsweise rechtsradikales Material oder gar Pornos in Umlauf bringen und dieses öffentlich bekannt wird.
- Es geht um den Schutz von Betriebsgeheimnissen, denn nur allzu oft wird per E-Mail und Internet Betriebsespionage betrieben.
- Und es geht auch ganz einfach darum, gezielte Informationen über einzelne unliebsame Individuen zu sammeln, die eine fristlose Kündigung oder - in weniger schweren Fällen - wenigstens eine Abmahnung als Maßregelung untermauern oder gar erst möglich machen.

Und diese Befürchtungen und Begründungen werden auch mit Zahlen belegt. So will eine Studie herausgefunden haben, dass 44% der US-Unternehmen mit mehr als 20.000 Mitarbeitern eigens Personal dazu abgestellt hat, um E-Mails mitzulesen oder andere Datenflüsse zu analysieren. 22% dieser Unternehmen haben dazu sogar spezielles Personal eingestellt<sup>2</sup>. In Unternehmen ab 1.000 Mitarbeitern sind die Zahlen noch nicht ganz so hoch: 36% dieser Unternehmen kontrollieren den E-Mail-Verkehr - Tendenz stark steigend.

Alle Befürchtungen der Arbeitgeber sind mit ein wenig Einfühlungsvermögen in die Interessenlage von Unternehmen zumindest nachvollziehbar, ihre Konsequenzen in vielen Situationen aber keinesfalls tolerierbar.

Aufklärung der Mitarbeiterinnen und Mitarbeiter über technische Überwachungsmöglichkeiten ist gefragt. Und die Forderung, dass beide Seiten mit offenen Karten spielen, um auf

<sup>1</sup> Wirtschaftsblatt-Online vom 9.9.2000 ([www.wirtschaftsblatt.at](http://www.wirtschaftsblatt.at))

<sup>2</sup> <http://www.heise.de/newsticker/meldung/108355>, 23.5.2008

der einen Seite niemanden „ins offene Messer“ laufen lassen, auf der anderen Seite aber die betriebliche Interessenslage zu schützen.

Denn die Überwachung im großen Stil ist bereits im Gange. Inzwischen werden fast 40% der PC-Arbeitsplätze in Unternehmen überwacht, sagt eine Umfrage der Steria-Mummert Consulting und des IT-Dienstleisters Inworks aus<sup>3</sup>. In den USA liegt diese noch weitaus höher und lag schon 2001 bei 63%<sup>4</sup>. Berechnet man mit ein, dass aufgrund kultureller Unterschiede die Bereitschaft in den USA, eine Überwachung zuzugeben, deutlich größer ist, dürften auch in Deutschland die genannten 40% ein eher schmeichelhafter Wert sein.

Doch nicht erst der eigentliche Einsatz, sondern schon alleine die Ankündigung der unternehmensweiten Installation von E-Mail- und Internet-Überwachungsprogrammen verändert das Surf-Verhalten der Angestellten dramatisch: Nach Aussagen von Carsten Rau, Geschäftsführer der ProtectCom, wird die Online-Zeit nach Ankündigung der Installation um bis zu 90% produktiver genutzt<sup>5</sup>.

Aber auch eigenverantwortliches Handeln der Mitarbeiter ist erforderlich: Regelungen zur Überwachung, Datenschutz und Internet-/E-Mail-Nutzung werden immer häufiger in Arbeitsverträgen, Betriebs- bzw. Dienstvereinbarungen oder Dienstanweisungen festgeschrieben - aber gut ein Fünftel der von Steria-Mummert befragten Personen weiß nicht, ob eine entsprechende Regelung existiert, und nur 25% geben an, explizite Regelungen zum privaten Surfverhalten zu haben. Genau diese Vereinbarungen sind es aber, die beiden Seiten Sicherheit geben und Wahrung der Interessen ermöglichen<sup>6</sup>.

---

<sup>3</sup> <http://www.stern.de/wirtschaft/arbeit-karriere/541157.html?eid=541941>, 17.4.2008

<sup>4</sup> Handelsblatt vom 16.7.2001 (www.handelsblatt.com)

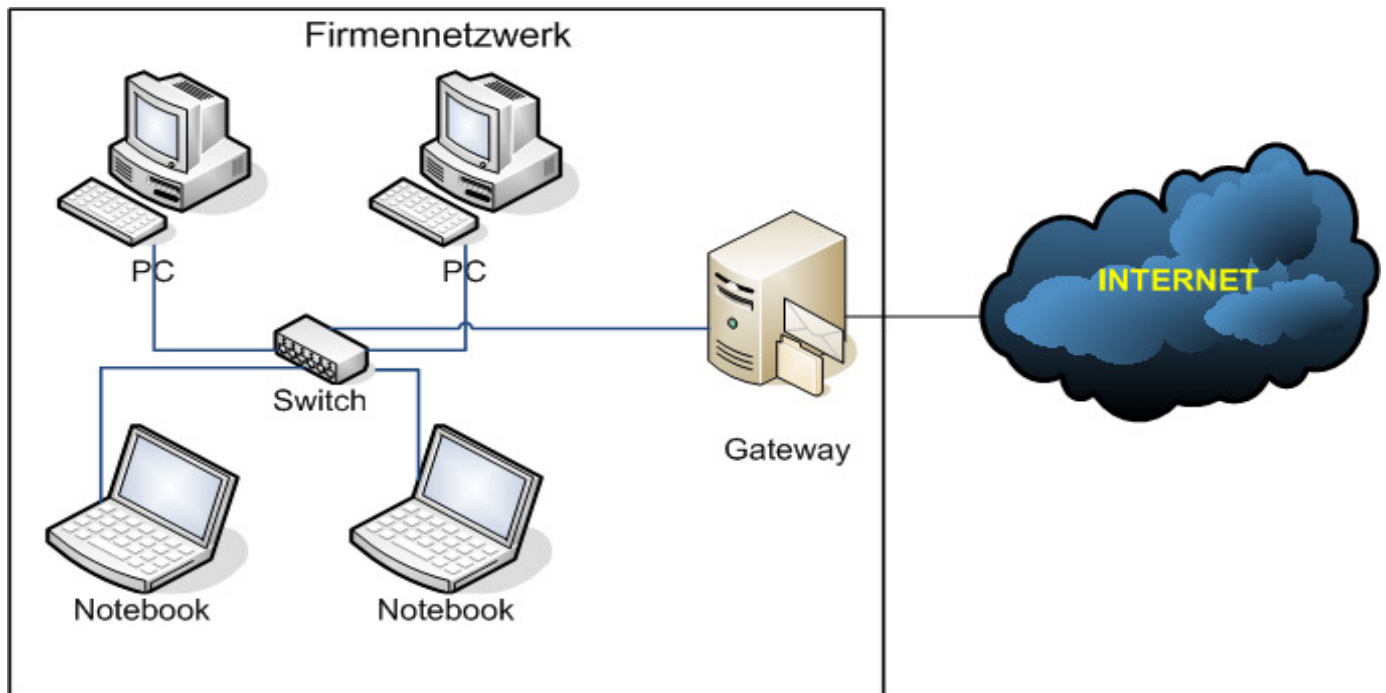
<sup>5</sup> Handelsblatt vom 16.7.2001 (www.handelsblatt.com)

<sup>6</sup> <http://www.stern.de/wirtschaft/arbeit-karriere/541157.html?eid=541941>, 17.4.2008

## Die technischen Grundlagen

Um zu verstehen, an welchen Stellen sich Angriffsmöglichkeiten für den großen oder kleinen Lauschangriff des Chefs ergeben, muss man verstehen, wie die Kommunikation von einem Firmennetzwerk in das Internet funktioniert.

Firmennetzwerke sind in aller Regel nach folgendem vereinfacht dargestellten Prinzip aufgebaut:



Jede Kommunikation aus einem Firmennetzwerk heraus mit dem Internet, sei es nun E-Mail, das WWW oder auch das Telefonieren über „Voice Over IP (VoIP)“ - erfolgt über eine zentrale Stelle: Das Gateway, die „Einfahrt“ in das weltweite Netz.

Dieses Gateway, das es in vielen verschiedenen Ausprägungen mit zahlreichen unterschiedlichen Funktionalitäten gibt - genannt seien hier nur die Schlagworte „Router“, „Firewall“ und „Proxy-Server“ - stellt die Verbindung zwischen den Netzen her und ist damit der Flaschenhals, den jede Information passieren muss.

Aus dieser sehr einfachen Darstellung heraus ergeben sich auch schon zwei prädestinierte Angriffspunkte zum Schnüffeln: Die einzelnen PCs im Unternehmen - im Allgemeinen nur für etwas plumpe und oftmals auch leicht zu erkennende Spionage-Attacken geeignet - und der zentrale Übergabepunkt zwischen den Netzen, wo man schon viel eleganter und sicherer vor Entdeckung lauschen kann.

Als Erstes sollen hier Möglichkeiten der Überwachung der PCs beschrieben werden. Die zentrale Überwachung am Übergabepunkt wird später erläutert.

## Die Überwachung am PC

### Gegen Gelegenheits-Lauscher kann man sich wehren

Viele Betriebssysteme und Anwendungsprogramme bringen selbst genügend Funktionen mit sich, die es Interessierten leicht möglich machen, eine Menge über den Benutzer und seine Surf- und E-Mail-Gewohnheiten zu erfahren. Allerdings ist das Auswerten der Informationen mühsam und nur zur gezielten Kontrolle einzelner Mitarbeiterinnen und Mitarbeiter geeignet, nicht aber zu einer unternehmensweiten oder gar präventiven Überwachung.

In vielen Fällen protokollieren Anwendungen die Benutzer-Aktivitäten mit, 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 Benutzers zu erhöhen und ihm bzw. ihr die Arbeit angenehmer zu machen (Cookies). Allen gemeinsam ist, dass diese Anwendungen die Informationen in Form von Dateien auf der lokalen Festplatte oder in einigen Fällen auf zentralen Firmen-Servern ablegen. Und alles, was in einem Netzwerk erst einmal als Datei existiert, ist durch Systemadministratoren und damit letztlich auch durch Vorgesetzte les- und auswertbar.

### *Setz dich und nimm dir 'nen Keks*

„Cookies“ sind schon seit ihrer Entwicklung durch die Firma Netscape - einst der Internet-Browser-Hersteller mit dem größten Marktanteil - immer wieder heftig diskutiert worden. Diese Diskussionen haben aber oftmals in erster Linie sicherheitstechnische Aspekte, da Cookies die bislang einzige direkte Möglichkeit sind, 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 bis heute aber nicht bestätigt hat, da es durch die reine Verwendung von Cookies noch niemandem gelungen ist, geheime Daten auszuspionieren oder zu löschen.

Der Zweck der Entwicklung von Cookies war eigentlich ein sehr edler: Durch das Speichern von Informationen auf dem lokalen Rechner war es erstmalig möglich, dass eine Internet-Seite einen Benutzer - oder zumindest dessen PC - „wiedererkennt“, was mit klassischen Internet-Techniken bisher nicht funktionierte.

Leider missbrauchen insbesondere Unternehmen aus der Branche der Internet-Werbung diese Cookies derart, dass sie unbedachte Benutzer bei ihrem Surfverhalten indirekt beobachten können. Sicherlich ein datenschutztechnischer Missstand, der aber an dieser Stelle nicht weiter ausgeführt werden soll.

Viel interessanter ist, dass Cookies schon bei einem flüchtigen Blick auf die Festplatte einiges über das Surfverhalten ihres Besitzers aussagen können. Beispielsweise schreibt der Internet-Explorer von Microsoft diese Cookies in Form von kleinen Dateien, die schon durch ihren Namen gewisse Gewohnheiten des Benutzers ausdrücken:

<code>gerrit_wiegand@ebay.com.txt</code>	geändert am 27.1.2008
<code>gerrit_wiegand@search.support.microsoft.com.txt</code>	geändert am 27.1.2008
<code>gerrit_wiegand@amazon.de.txt</code>	geändert am 27.1.2008

Ein Leichtes zu erraten, was hier an besagtem Tag so alles getan wurde...

Wenn man diese Dateien öffnet - das geht ganz leicht mit einem beliebigen Texteditor oder Schreibprogramm - offenbaren sie oft noch mehr Details, beispielsweise welche Kate-

gorie von Bildern ich besonders bevorzuge, wie oft ich schon Suchanfragen in einer Suchmaschine gestellt habe oder ähnliches - je nach Geschmack und Geschick des Programmierers und nach Sammelwut des Internet-Anbieters.

Das ist allerdings keine Besonderheit von Microsoft, sondern alle gängigen Browser legen diese Cookies in mehr oder weniger leicht zugänglicher Form ab.

Wie man Cookies findet, wie man sie sich ansehen kann und wie man sie verbietet

Unter Windows 2000/XP legt der Internet-Explorer die Cookies standardmäßig im Verzeichnis `c:\Dokumente und Einstellungen\Benutzername\cookies\`. Für jedes Cookie wird dabei eine eigene Datei erzeugt.

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 `*cookie*` ein. So werden Sie schnell entweder die Datei selbst oder aber den entsprechenden Ordner finden.

Wenn Sie die Dateien erst einmal gefunden haben, reicht meist ein Doppelklick, um sie zu öffnen. Wenn das nicht funktionieren sollte, merken Sie sich den angezeigten Pfad zu den Dateien, öffnen Sie einen Texteditor (wählen Sie dazu im Startmenü den Menüpunkt „Ausführen“ und geben Sie dort `notepad` ein) und öffnen Sie die Cookie-Datei durch das Menü „Datei / Öffnen“.

Um das Anlegen von Cookies in Zukunft zu verbieten oder einzuschränken, wählen Sie im Internet-Explorer Einstellungen unter „Extras“, „Internetoptionen“, „Datenschutz“ und dann dem Schalter „Erweitert“. In den beiden genannten Menüs finden Sie außerdem noch jede Menge anderer interessanter Einstellungen zur Datensicherheit und zum Datenschutz.

Glücklicherweise lässt sich diese Art der Protokollierung des Surf-Verhaltens recht einfach unterbinden: Weder der Browser noch die meisten Internet-Seiten nehmen es Ihnen übel, wenn Sie die Dateien einfach löschen! Schlimmstenfalls werden Sie beim nächsten Besuch der Seite einfach nicht wiedererkannt.

Und um in Zukunft diese wohl einfachste Methode der Surf-Kontrolle zu vermeiden, können Sie in allen heute gängigen Browsern das Schreiben von Cookies explizit verbieten (siehe Kasten) - vorausgesetzt, Ihr Netzwerk-Administrator hat Ihnen nicht das Recht entzogen, diese Einstellungen zu ändern. Dann hilft nur, regelmäßig die genannten Dateien zu löschen.

Ein wenig eleganter geht es mit sogenannten Paranoia-Programmen, wie beispielsweise dem gerade in einer neuen Version erschienenen „Internet-Cleanup“ der Firma Ontrack<sup>7</sup> oder auch diversen kostenlosen Programmen aus dem Internet (beispielsweise Crap Cleaner von Wedigo<sup>8</sup>), die Ihnen das Löschen von Cookies und anderen verräterischen Protokollierungen automatisch abnehmen. Aber auch nur, wenn Sie diese Programme installieren dürfen, was auf Arbeitsplatz-Rechnern oftmals nicht erlaubt ist.

<sup>7</sup> [www.ontrack.de](http://www.ontrack.de)

<sup>8</sup> [www.ccleaner.de](http://www.ccleaner.de)

## **Cache as Cache can**

Der „Cache“ ist ein Verzeichnis auf dem PC oder in manchen Unternehmensnetzwerken auch auf einem zentralen Server, in dem die Inhalte von bereits besuchten Internet-Seiten zwischengespeichert werden. Diese Technik wurde ein erster Linie entwickelt, um die Netzwerke zu entlasten und Informationen, die zu einem früheren Zeitpunkt bereits aus dem Internet abgerufen wurden, nicht erst wieder erneut aufwändig herunterzuladen zu müssen, sondern sie viel schneller von der Festplatte zu holen.

Dabei sammelt sich im Cache ein wahrer Pool von persönlichen Surf-Gewohnheiten. Praktisch jedes Bild und die meisten Inhalte der besuchten Seiten werden für einen gewissen Zeitraum - zwischen wenigen Stunden und mehreren Wochen - zwischengespeichert und können ohne jeden Aufwand angesehen werden.

Ein Blick in die entsprechenden Verzeichnisse offenbart alle Inhalte.

Aber auch dagegen kann man sich wie bei Cookies sehr einfach schützen: Den Cache ausschalten, was jedoch das Surfvergnügen wegen der wesentlich geringeren Übertragungsgeschwindigkeit deutlich schmälert, oder durch das regelmäßige manuelle Löschen der Dateien oder wieder durch den Einsatz der oben genannten Paranoia-Programme.

### Den Cache finden, ansehen und löschen

*Unter Windows 2000/XP legt der Internet-Explorer alle gecachten Dateien standardmäßig im Verzeichnis `c:\Dokumente und Einstellungen\Benutzername\Lokale Einstellungen\Temporary Internet Files\`.*

*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: Im Internet-Explorer unter „Extras“, „Internetoptionen“, „Allgemein“ und dann „Einstellungen“.*

## **Spion wider Willen**

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 Benutzerinnen 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 Such-

funktion (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 Systemadministrator 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.

## Schuldig!

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.

## 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 Systemadministrator) 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 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 Administrator 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<sup>9</sup>. Bereits im September waren in Deutschland rund 4.500 Installationen vorhanden, mit einer Verschiebung der Unternehmensnutzung hin zu 75%<sup>10</sup>. Weltweit wurde Spector - nur ein Programm von vielen! - bisher über 70.000 Mal verkauft<sup>11</sup>.

<sup>9</sup> Telepolis vom 9.5.2001 ([www.heise.de/tp/](http://www.heise.de/tp/))

<sup>10</sup> Financial Times Deutschland vom 18.9.2001 ([www.ftd.de](http://www.ftd.de))

<sup>11</sup> Financial Times Deutschland vom 18.9.2001 ([www.ftd.de](http://www.ftd.de))

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

Name	Hersteller	Beschreibung <sup>12</sup>
Spector Pro V6	ProtectCom (www.protectcom.de)	<ul style="list-style-type: none"> <li>○ Ursprünglich in den USA für den privaten Markt entwickelt. Inzwischen auch in Deutschland verfügbar (über 5.000 Installationen) und überwiegend in Unternehmen eingesetzt.</li> <li>○ Protokolliert: <ul style="list-style-type: none"> <li>○ Alle Tastenanschläge,</li> <li>○ alle besuchten Internet-Seiten,</li> <li>○ alle Chat-Unterhaltungen,</li> <li>○ alle Mails und Instant-Messaging-Aktivitäten (ICQ, MS-Messenger etc.),</li> <li>○ alle Bildschirmmasken (Screenshots) mit Wiedergabefunktion als „Videofilm“ und automatischer Analyse der Bilder.</li> </ul> </li> <li>○ Läuft wahlweise im sichtbaren oder unsichtbaren Modus.</li> <li>○ Speicherung der Protokolle und Bilder auf der lokalen Festplatte.</li> <li>○ Durch die Hinterlegung von Schlüsselwörtern und Phrasenlisten kann bei Eingabe der entsprechenden Wörter eine automatische E-Mail generiert werden („Alarmpfunktion“).</li> <li>○ Ausgezeichnet mit dem „BigBrother Award 2001 für Überwachung am Arbeitsplatz“<sup>13</sup>.</li> <li>○ Preis: ca. 85 € pro Installation.</li> </ul>
IamBigBrother	(www.iambigbrother.com)	<ul style="list-style-type: none"> <li>○ Überwiegend für den Einsatz im privaten Bereich entwickelt.</li> <li>○ Protokolliert: <ul style="list-style-type: none"> <li>○ Alle verwendeten Programme,</li> <li>○ alle besuchten Internet-Seiten,</li> <li>○ alle E-Mails,</li> <li>○ alle Tastenfunktionen,</li> <li>○ alle Bildschirmmasken (Screenshots).</li> </ul> </li> <li>○ Bietet zusätzlich eine Filter-Funktion, mit der der Aufruf von festgelegten Internet-Seiten gleich unterbunden werden kann.</li> <li>○ Speichert die Daten auf der lokalen Festplatte.</li> <li>○ Preis pro Installation: ab ca. 40 €.</li> </ul>
All In One Keylogger	RelyTec	<ul style="list-style-type: none"> <li>○ Speichert alle Tastatureingaben (Key Logger).</li> <li>○ Nimmt Instant Messenger auf.</li> <li>○ Überwacht Nutzung von Anwendungen</li> <li>○ Nimmt Desktop-Aktivität auf.</li> <li>○ Nimmt Screenshots auf.</li> <li>○ Schnelle Suche über das Protokoll.</li> <li>○ Sendet Berichte per E-Mail, FTP-, Netzwerk.</li> <li>○ Nimmt Gespräche über das angeschlossene Mikrofon im Computer auf.</li> <li>○ Erstellung von HTML-Berichten.</li> <li>○ Deaktiviert Anti Keylogger Programme.</li> <li>○ Deaktivierung unerwünschter Software.</li> <li>○ Filter zum Überwachen von bestimmten Benutzer-Accounts.</li> <li>○ Diaschau von aufgenommenen Screenshots.</li> </ul>

<sup>12</sup> Wenn nicht anders angegeben: Herstellerangaben

<sup>13</sup> www.bigbrotherawards.de

		<ul style="list-style-type: none"> <li>○ Sendet Berichte per FTP.</li> <li>○ Sendet Berichte im HTML-Format.</li> <li>○ Blockiert unerwünschte URLs.</li> <li>○ Stoppt die Protokollierung, wenn sich Computer im Ruhezustand befindet.</li> <li>○ Neu - Nicht sichtbar im Task-Manager (98/ME/2000/2003/XP/Vista).</li> <li>○ Nimmt Mauszeigeraktivität auf.</li> </ul>
--	--	--

### **... und wie man sich dagegen wehrt**

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 Benutzer aufmerksam machen könnten (vielsagende Dateinamen, Tray-Icons, Pop-up-Fenster etc.).

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.

Die meisten Key-Logger legen die gesammelten Daten und Bildschirmfotos zumindest zeitweise auf der lokalen Festplatte ab. Damit sind sie ähnlich leicht zu entdecken wie die weiter oben erwähnten allgemeinen Log-Protokolle.

Wer sich unsicher fühlt, ob er 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<sup>14</sup> oder den einschlägigen Datenschutzes-Seiten<sup>15</sup>, was es mit diesen speziellen Dateien auf sich hat.

<sup>14</sup> Beispielsweise `de.comp.security` (eher technische Diskussionen) oder `de.soc.datenschutz`. Wenn Sie keinen Zugriff auf ein News-Programm haben, finden Sie diese Gruppen auch unter <http://groups.google.com>

<sup>15</sup> Beispielsweise das virtuelle Datenschutz-Büro unter <http://www.datenschutz.de>

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.

## Die zentrale Überwachung

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, VoIP 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.

- 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 Benutzer aus dem Internet Programme herunterladen darf, ob er 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.
- 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.
- 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 Benutzern 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.

## Kein Kraut gewachsen

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.

Die Probleme:

- In vielen Fällen sind sich die Anwender nicht bewusst, dass solche Protokollierungen stattfinden und haben ein entsprechend unbedarftes Surf- und E-Mail-Verhalten.
- Als Anwender kann man praktisch nicht herausfinden, was genau protokolliert wird und wie bzw. ob die Protokolle ausgewertet werden.
- Die ohnehin vorhandenen Datenbestände verleiten Vorgesetzte oder Administratoren leicht dazu, den Kollegen „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 A eine Mail an Anwender 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.

## Der Spion im Server

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 von der Überwachung erfahren. Denn der Einsatz solcher Spionage-Software kann „mit Bordmitteln“ praktisch nicht entdeckt werden.
- Das ist sicherer, da Benutzerinnen 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 Benutzers - fast in die Viren-Kategorie der „Trojanischen Pferde“ eingeordnet werden<sup>16</sup>.

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.

Einer der größten Anbieter solcher „Spionage-Software“ ist die Firma Websense mit ihrem gleichnamigen Produkt Websecurity Suite.

Websense beschäftigt einen ganzen Stab von Mitarbeitern, 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 Mitarbeiter in seiner Arbeitszeit aufruft und die zu dieser Zeit für ihn gesperrt ist, in der Freizeit aber zugänglich sein soll, kann in einer speziellen Liste erfasst werden. Dieses Portal kann der Mitarbeiter 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 wird beispielsweise bei der Firma XEROX für die Überwachung von 92.000 Mitarbeitern und Mitarbeiterinnen eingesetzt und auch die US-Army hat diese Software ange-

---

<sup>16</sup> Als „Trojanische Pferde“ werden Programme bezeichnet, die im Allgemeinen eine „Nutz-Funktion“ besitzen, also etwas, das der Anwender 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.

lich für 200.000 Arbeitsplätze lizenziert. Insgesamt gibt Websense die Anzahl der Lizenzen auf über 5 Millionen in über 8.400 Unternehmen an<sup>17</sup>.

Neben den Internetzugriffen überwacht die Websecurity Suite auch den gesamt 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 E-Mails 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.

Name	Hersteller	Beschreibung <sup>18</sup>
Websense	Websense (www.websense.com)	<ul style="list-style-type: none"> <li>○ Filtert alle WWW-Zugriffe.</li> <li>○ Die zu filternden Internet-Seiten werden zentral von Websense gepflegt und von Menschen kategorisiert.</li> <li>○ Beschränkung der Zugriffe kann generell erfolgen oder beispielsweise nach Kategorien („Spiele“, „Online-Banking“ o.ä.), Volumen (zeitlich oder kapazitiv) oder sonstigen Regeln.</li> <li>○ Bietet detaillierte Auswertungsmöglichkeiten und Alarm-Funktionen an.</li> <li>○ Nutzfunktionen: Benutzerabhängige Internet-Rechte können einfach festgelegt werden (zeitlich, volumenabhängig). Auch können unterschiedliche Einstellungen für „während der Arbeitszeit“ und „nach der Arbeit“ vorgenommen werden.</li> </ul>
WebSpy	ProtectCom (www.protectcom.de)	<ul style="list-style-type: none"> <li>○ Filtert alle Internet-Zugriffe (auch andere Dienste als WWW wie bspw. FTP, Instant-Messaging, Chat) auf Basis von Schlagwort-Listen.</li> <li>○ Ermöglicht die Festlegung von Internet-Richtlinien.</li> <li>○ Umfangreiche Protokollierungs- und Alarm-Funktionen (Module „Sentinel“ und „Analyzer“).</li> <li>○ Datenbankgestützte (und damit effektive) Protokollierung und Auswertung.</li> </ul>
Internet-Watcher 2000	Bernard D&G (www.internetwatcher.de)	<ul style="list-style-type: none"> <li>○ Filtert alle WWW-Zugriffe auf Basis von Schlagwort-Listen, überwiegend für den privaten Einsatz entwickelt.</li> <li>○ Beschränkung der Zugriffe kann „On the Fly“ erfolgen, d.h. es können Internet-Seiten, auf denen bestimmte Schlagworte stehen, automatisch per Passwort geschützt werden.</li> <li>○ Bietet detaillierte Auswertungsmöglichkeiten.</li> <li>○ Nutzwert: Ist gleichzeitig ein Internet-Proxy zum Zugriff mehrerer Rechner auf einen Internet-Anschluss. Enthält weitere Funktionen wie Werblocker zur Beschleunigung des Seitenaufbaus und Cookie-Filter.</li> </ul>

<sup>17</sup> [www.xenia-systems.de/websense.htm](http://www.xenia-systems.de/websense.htm)

<sup>18</sup> Wenn nicht anders angegeben: Herstellerangaben

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.

### *... und wie man sich dagegen wehrt*

Wie eingangs bereits gesagt: Normale Benutzerinnen 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 vom Systemadministrator „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.

### 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.

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“ Anwender 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 berechtigte Empfänger, der 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 Schlüsseln 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 Empfängers noch aktuell ist, der Empfänger 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 Empfänger 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 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 Benutzers 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 sicherlich die beste und sicherste 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.pgpI.org/> kostenlos downloaden.

## 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, die 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.

## 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-Protokoll 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!

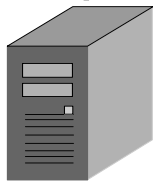
Der zweite Modus ist aufwändiger einzurichten, liefert aber dafür die Möglichkeit des absolut anonymen Surfens aus Unternehmensnetzwerken heraus!

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<sup>19</sup>, 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.

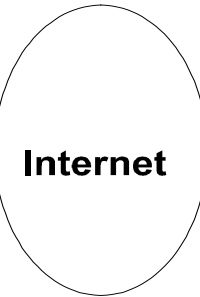
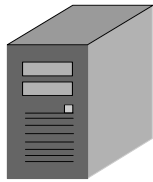
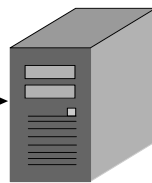
---

<sup>19</sup> Mehr dazu finden Sie auf den Seiten von HTTPPort unter [www.htthost.com](http://www.htthost.com) im Bereich „HTTPPort / FAQ“

**Methode 1:****Arbeitsplatz-PC****Gateway**

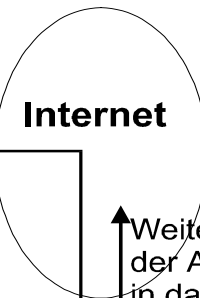
↔  
Unverschlüsselte  
Anfrage auf dem  
HTTPS-Port

↔  
Umwandlung des  
HTTPS-Ports  
bspw. auf den  
FTP-Port

**Methode 2:****Arbeitsplatz-PC****Gateway**

↔  
Verschlüsselte  
Anfrage auf dem  
HTTPS-Port

↔  
"direkte"  
Verbindung  
zum HTTPPort 3-  
Server



↕  
Weiterleitung  
der Anfrage  
in das internet

**HTTPPort 3-  
Server**

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 Port 80 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 abgibt 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 JAP-Forschungsgruppe über „Test-Benutzer“ sehr erfreut.

Allerdings muss man hier ein wenig Pioniergeist mitbringen.

## Fazit

Wie eingangs gesagt: DIE Methode zur anonymen Internet-Nutzung gibt es nicht! JAP und HTTPPort liefern interessante Ansätze, haben sich aber noch nicht großflächig durchgesetzt oder befinden sich noch in der Entwicklung. PGP 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 Lauschern wenigstens ein wenig schwerer zu machen und ansonsten nur auf der Hut sein. Aber vielleicht hat die Darstellung der Möglichkeiten, wie „der Chef mitsurfen“ kann, ja auch ein wenig sensibilisiert und sorgt für einen verantwortungsvolleren Umgang mit dem Internet.