Präs: 13. Juli 2004 Nr.: 2223/J-BR/2004

Anfrage

der Bundesräte Prof. Konecny
und GenossInnen

betreffend Einsatz von Schnüffelsoftware in öffentlichen Dienststellen der Republik Österreich

an den Bundesminister für soizale Sicherheit, Generationen und Konsumentenschutz

In der aktuellen Online-Ausgabe der Computerwoche (www.computerwoche.de) ist unter Produkte/Technologien folgender Artikel publiziert:

Schnüffelsoftware spioniert PC-Anwender aus

Von CW-Redakteur Martin Seiler.

MÜNCHEN (COMPUTERWOCHE) - Big Brother is watching you! Mittels Spyware können Unbefugte detailliert überwachen, was Anwender an ihrem PC tun, und auf diese Weise auch Firmeninterna ausspionieren. Doch es gibt Tools, mit denen die Schnüffelprogramme gefunden und entfernt werden können.

Niemand lässt sich gern auf die Finger schauen. Leider gibt es jedoch immer wieder Personen, die es brennend interessiert, was andere an ihren heimischen PCs oder den Rechnern im Büro tun. Sogenannte Spyware befriedigt diese Neugier, der von vielen gefürchtete gläserne Anwender wird damit zur Realität.

Glaubt man einschlägigen Untersuchungen, können sehr viele bereits Opfer sein, ohne es zu wissen: So fanden der US-amerikanische Provider Earthlink und der Sicherheitsanbieter Webroot Software heraus, dass jeder dritte PC mit Spyware-Programmen verseucht ist. Für ihren "Spy Audit Report" haben die beiden Unternehmen eigenen Angaben zufolge bei zirka 1,5 Millionen PC-Scans mehr als 500.000 Spyware-ähnliche Programme gefunden, die auf den Rechnern mit oder ohne Kenntnis der Benutzer installiert wurden. Fast 134.000 von mehr als 420.000 allein im April überprüften Rechnern enthielten einen Trojaner oder ein Systemüberwachungs-Tool, etwa einen Keylogger.

Zu ähnlichen Ergebnissen kommen andere Untersuchungen. So wollen die Analysten von Harris Interactive bei einer im Auftrag des Herstellers Websense gestarteten Telefonumfrage unter US-amerikanischen IT-Experten im Frühjahr herausgefunden haben, dass 29 Prozent aller Rechner mit Spyware infiziert sind. Die Unternehmensberatung Mummert Consulting warnte im September 2003, dass jeder dritte Computerarbeitsplatz in deutschen Unternehmen mit Hilfe entsprechender technischer Maßnahmen überwacht wird. Und aus dem Pest Research Center des Herstellers Pestpatrol ist zu hören, dass über 85 Prozent aller deutschen Unternehmen mit Spionageprogrammen infiziert sein sollen. Die Gesamtzahl der im Umlauf befindlichen Überwachungsprogramme sei von Dezember 2003 bis März 2004 von 290.000 auf fast 550.000 angestiegen.

Diese Zahlen klingen drastisch, relativieren sich jedoch, wenn man bedenkt, dass es unterschiedliche Arten von Spyware gibt. Allgemein gesprochen handelt es sich dabei um Programme, die es ermöglichen, das Verhalten eines PC-Benutzers zu überwachen und anschließend auszuwerten. Die Bandbreite reicht dabei von einfachen Browser-Cookies über entsprechende Funktionen innerhalb von werbefinanzierten Hilfsprogrammen bis hin zu spezialisierten Lösungen, die entweder einzelne Aktivitäten wie zum Beispiel Tastatureingaben kontrollieren oder die komplette Überwachung eines Rechners und aller daran stattfindenden Aktivitäten erlauben.

Oliver Pott, Geschäftsführer von Pestpatrol Deutschland, räumt ein, dass nur sieben bis acht Prozent der Spionageprogramme zur höchsten Gefährdungsklasse gehören. Das Gros der Schnüffler stellen Cookies dar, die aufzeichnen, wann ein User welche Web-Seiten besucht und welche Inhalte er dabei aufruft.

Einen Schritt weiter geht so genannte Adware, also mittels Werbung finanzierte Programme: Diese beschränken sich häufig nicht darauf, dem Benutzer hin und wieder ein paar Produkteinblendungen zuzumuten, sondern sammeln wie die Software des Unternehmens Gator, das inzwischen unter Claria firmiert, Daten über das Surfverhalten der User und verkaufen diese Informationen an die Werbekunden weiter. Der Hersteller nennt dies selbstbewusst "Online-behavioural Marketing", was so viel heißt wie am Online-Verhalten des Surfers

orientiertes Marketing. Auch die Client-Software der Internet-Tauschbörse "Kazaa" sammelt fleißig Informationen über ihre Benutzer und übermittelt diese zur Auswertung und Weiterverarbeitung über das Internet an spezielle Server.

Der Anbieter Webroot warnt, dass Adware Komponenten auf dem Rechner installiert, die persönliche Informationen, beispielsweise über das Alter, Geschlecht, Wohnort, Kaufinteressen oder Surfgewohnheiten sammeln. Häufig sind nur versteckt in den Nutzungsbedingungen der Software Hinweise darauf zu finden, dass überhaupt Spyware installiert wird. Der zumeist ahnungslose Mitarbeiter kann sich daher nicht erklären, woher die plötzliche Flut von Popup-Einblendungen kommt, warum sein System langsamer läuft und auch die Netzverbindung schlechter ist als sonst.

Die bei weitem gefährlichste Spyware-Kategorie bilden jedoch Tools, die sich unter Oberbegriffen wie Systemüberwachung oder Aktivitäts-Monitoring zusammenfassen lassen. Dazu gehören etwa Keylogger, die sämtliche Tastatureingaben erfassen und in eine Datei speichern. Diese kann von einem Angreifer später ausgewertet und beispielsweise auf darin enthaltene Passwörter, Kreditkartennummern oder sonstige sensible Informationen untersucht werden. "Keylogger stellen einen relativ hohen Anteil innerhalb der Spyware dar", warnt Experte Pott. Inzwischen verbreiten sich Keylogger auch über Viren und Würmer: "Fizzer" (Mai 2003), "Bugbear.B" (Juni 2003) und "Mydoom" (Januar 2004) enthielten alle ein entsprechendes Modul, das auf den infizierten Rechnern installiert wurde.

Eine andere Form der Überwachung ermöglicht das im Internet verfügbare Programm "Soundsnooper": Einmal installiert, überwacht es die Soundkarte des PC und beginnt automatisch mit der Aufzeichnung, sobald über das dazu notwendige Mikrofon Sprache wahrgenommen wird. Um Festplattenplatz zu sparen, stoppt die Aufnahme, sobald es ruhig ist. Der Anbieter nennt als Anwendungsmöglichkeiten unter anderem das Aufzeichnen von Konferenzen, das Mitschneiden von Telefonaten sowie das Überwachen von Mitarbeitern.

Neben diesen auf bestimmte Funktionen spezialisierten Tools gibt es aber auch Produkte, die fast alle Aktivitäten an einem PC überwachen und dokumentieren können. Dazu gehören unter anderem "System Recon", "Surf Spy" (von dem es auch eine Enterprise-Version gibt), "Eblaster", "Farsighter", "Realtime Spy", "Spy Agent", "Actmon", "Orvell", "Spector" oder "Winston". Einige dieser Werkzeuge erfassen nahezu alles, was am PC geschieht. Zum Standard zählt neben dem Protokollieren der Tastaturanschläge, der aufgerufenen Anwendungen und der besuchten Web-Seiten das Anfertigen von Screenshots in einem festgelegten Intervall (siehe Kasten "Spyware-Arten"). Auch Chat-Sessions, E-Mail-Verkehr oder Instant Messaging lassen sich aufzeichnen, einzelne Lösungen können sogar so konfiguriert werden, dass sie nur bei bestimmten Schlüsselwörtern aktiv werden.

Die Programme können zumeist völlig unsichtbar im Hintergrund laufen, so dass das Opfer bis auf eine etwas längere Antwortzeit seines Rechners nichts von der Überwachung merkt. Die gesammelten Daten können entweder automatisch per E-Mail versendet oder aber über das lokale Netz auf einem Server gespeichert werden, von wo aus sich dann Auswertungen starten und umfassende Reports erstellen lassen. Auf Wunsch blenden Produkte wie etwa Actmon Fenster ein, die den PC-Benutzer auf die Überwachung hinweisen - eine Funktion, die besonders beim offiziellen Einsatz in Unternehmen interessant sein dürfte.

Orvell, Spector und Winston sind über das in Saarbrücken ansässige Unternehmen Protectcom erhältlich. Dessen Geschäftsführer Carsten Rau nimmt kein Blatt vor den Mund, wenn er über die Produkte spricht: "Überwachungssoftware hat sich etabliert, und wir haben kein Problem damit, deutlich zu sagen, was unsere Software tut".

Der Erfolg des Unternehmens scheint ihm Recht zu geben: Nachdem Protectcom im Jahr 2002 rund 7000 Lizenzen verkaufte, durften sich Rau und sein Team im darauf folgenden Jahr über eine Zunahme des Geschäfts um 75 Prozent freuen. Auch in diesem Jahr liege das Wachstum "im zweistelligen Bereich". Anrüchig ist die Spionagesoftware aus Sicht von Rau auch deshalb nicht, **weil inzwischen neben Privatkunden immer mehr Unternehmen, Behörden und offizielle Stellen wie das österreichische Bundeskanzleramt derartige Tools kaufen und einsetzen.**

Auch das Staatsarchiv Münster gehört zu den Kunden des Herstellers. In der Landesbehörde ist der "Webspy Analyzer" im Einsatz, um zu kontrollieren, welche Web-Seiten die Mitarbeiter besuchen. Wie Christian Wortmann, zuständig für die Netzwerkverwaltung und die Anwenderbetreuung, erzählt, wird jeden Monat das Surfverhalten von zwei nach dem Zufallsprinzip ausgewählten Mitarbeitern mit Hilfe des Tools untersucht. "Wir wollen nicht den Big Brother spielen, aber dennoch eine Möglichkeit der Kontrolle haben", erzählt der Spezialist, demzufolge die Überwachung "auf einem niedrigen Level" stattfindet. Der Einsatz der Software wurde den Mitarbeitern vorher mitgeteilt, außerdem sichert eine Dienstvereinbarung die Auswertung rechtlich ab.

Programme wie Orvell, Eblaster oder Actmon laden natürlich zu Missbrauch ein, was die Hersteller auch bereitwillig zugeben. Sie weisen auf ihren Internet-Seiten immer wieder darauf hin, dass hierzulande niemand ohne seine Zustimmung überwacht werden darf. Mathias Roth, Vice President von iOpus Software, dem

Hersteller von Actmon, glaubt an die richtige Positionierung und verantwortungsvolle Werbung als ein Mittel, um Missbrauch vorzubeugen: "Wir sehen unsere Software vor allem als Werkzeug für Systemadministratoren und den technischen Support und bewerben sie auch entsprechend." Werbung im Stil von "Spionieren Sie Ihrem Gatten hinterher" sei für das Unternehmen daher tabu.

Von Actmon ist derzeit eine neue Version in Vorbereitung, die im Sommer erscheinen soll. Diese wird Roth zufolge die Möglichkeit bieten, auch Aktivitäten wie das Löschen oder Kopieren von Dateien auf einem Rechner zu protokollieren. Außerdem könne die Software dann auch feststellen, wenn der Rechner via Netzwerk oder USB-Stick "angezapft" wird. Roth sieht in dieser Funktion "eine Art Intrusion Detection für das Frontend".

Fazit

Leider arbeiten nicht alle Reinigungs-Tools immer 100-prozentig zuverlässig: So haben Tests gezeigt, dass beispielsweise weder Spybot S&D noch Spy Sweeper momentan in der Lage sind, Actmon zu erkennen. Im Zweifelsfall hilft also nur der Rückgriff auf ein Werkzeug wie Wintasks 4 Professionals.

Dem Manager zufolge sind es in erster Linie Firmen, die sich die Software zulegen: Derzeit interessieren sich überwiegend Kunden aus Nordamerika (USA und Kanada) für Actmon, in Europa und Asien sei jedoch eine steigende Nachfrage zu beobachten. Auf das Einsatzgebiet der Software angesprochen, gibt der Manager das Überwachen sicherheitsrelevanter PCs oder - bei einem konkreten Verdachtsfall - einzelner Mitarbeiter an. Protectcom-Mann Rau zufolge ist es mit Hilfe des Tools schon mehreren Unternehmen gelungen, Mitarbeiter zu überführen, die firmeninterne Informationen an die Konkurrenz weitergeleitet haben.

In Fällen wie diesen ist der Einsatz von Überwachungs-Tools also durchaus sinnvoll. In vielen anderen Situationen haben jedoch nicht nur einzelne Mitarbeiter im Unternehmen, sondern auch die für die Sicherheit zuständigen IT-Experten aus Gründen der Geheimhaltung beziehungsweise Spionageabwehr ein Interesse daran, Spyware zu finden und zu entfernen. Diese kann schließlich auch von einem externen Angreifer in das Netz geschleust worden sein. Der US-amerikanische Sicherheitsexperte Marcus Ranum kritisiert im jüngsten Sicherheits-Newsletter des System-Administration-, Networking- and Security-(SANS-) Institute, dass die IT-Abteilungen dieses Problem viel zu lange ignoriert haben: "Ein Elefant lässt sich nicht unter den Teppich kehren."

Wer einen Rechner von Spionagesoftware befreien will, kann dazu Spezial-Tools wie "Wintasks 4 Professionals" benutzen. Diese Lösung bietet umfangreiche Analysefunktionen, die weit über das Leistungsvermögen des Windows-eigenen "Task Managers" hinausgehen und dem Anwender selbst im Hintergrund verborgen laufende Prozesse und Anwendungen anzeigen. Diese lassen sich dann gezielt beenden, ungewünschte Programme können dauerhaft aus dem System entfernt werden. Allerdings erfordert die Bedienung dieser Software spezifische Systemkenntnisse und ist zudem zeitraubend. Leichter geht es mit speziellen Tools, die den Rechner untersuchen und Schnüffelprogramme deinstallieren.

Eine ganze Reihe von Anbietern hat sich inzwischen auf solche Spyware-Entferner spezialisiert. Ähnlich wie Virenschutzprogramme benutzen diese Lösungen Signaturen, anhand derer sie datensammelnde Eindringlinge entlarven. In der Regel lassen sich verdächtige Anwendungen zunächst isolieren, bevor sie in einem weiteren Schritt dauerhaft vom System gelöscht werden. Zu den bekanntesten Vertretern dieser Gattung gehören "Spybot Search & Destroy", "Spy Sweeper" oder "Pestpatrol".

Im Internet finden sich zudem kostenlose Utilities zur Überprüfung des Rechners, etwa "Elbtecscan" des Hamburger Softwarehauses Elbtec GmbH. Dieses kompakte Werkzeug ist jedoch insofern eingeschränkt zu benutzen, als es lediglich Spector, Eblaster und Orvell erkennt. Der Hersteller Pestpatrol bietet unter www.pestscan.de einen Online-Service, der den Rechner auf Schnüffel-Tools untersucht.

Speziell für Unternehmen, die sicherstellen wollen, dass niemand Unbefugtes den eigenen Mitarbeitern bei der Arbeit über die Schulter sieht, bietet sich Version 5.5 von "Pestpatrol" an. Die Software ist Server-basiert, und lässt sich von dort auf den Arbeitsplatzrechnern der Mitarbeiter installieren. Von einer zentralen Konsole aus können Administratoren dann den virtuellen Kammerjäger durchs Netz schicken und die elektronischen Spione von den Rechnern ihrer Mitarbeiter entfernen lassen. Auch Websense macht mit "Websense Enterprise" Jagd auf die Schnüffelsoftware. Dabei wird der Datenverkehr im Netz mit Hilfe spezieller Algorithmen gefiltert.

Bei den Produkten, die das Unternehmen Protectcom anbietet, und welche scheinbar auch vom österreichischen Bundeskanzleramt angekauft wurden, handelt es sich z.B. um:

13. Juli 2004

Orvell Monitoring

Entworfen zur Aufnahme aller Computeraktivitäten.

- *jeder Tastenanschlag*
- *jede Internetseite & jeder Chat*
- *jede Anwendung und jede eMail*

Auch für AOL

Produktservice

Unverbindliche Beratung per Telefonhotline (Montag-Freitag) oder per eMail.

Computer Bild Ausgabe 13/2004

Produktinformationen zu Orvell Monitoring 2004

Home Info Kaufen Presse Fragen System Screenshot

Weitere Informationen zu Orvell Monitoring 2004

Orvell Monitoring kombiniert viele Monitoringtools in einem Programm: permanente Aufzeichnung aller Bildschirminhalte (auch eMails und Chat-Unterhaltungen), Aufzeichnung aller besuchten Internetseiten, aller Tastenanschläge (Keylogger) und aller gestarteten Programme. Orvell Monitoring verfügt ebenfalls über ein intelligentes und sofortiges eMail-Warnsystem nach Ihren persönlichen Einstellungen: Sie werden auf Wunsch sofort informiert, sobald bedenkliche Aktivitäten erkannt werden.

Was nimmt Orvell Monitoring auf?

Wie eine Überwachungskamera tätigt Orvell Monitoring regelmäßige Aufnahmen des Bildschirms (z.B. alle 30 Sekunden). Die Aufnahmen werden versteckt und komprimiert auf Ihrer Festplatte abgelegt. Einige Sekunden später nimmt Orvell Monitoring das nächste Bild auf. Sie entscheiden, wie häufig und detailliert (Farbe oder Schwarz Weiß, hohe oder niedrige Qualität) Orvell Monitoring aufnehmen soll. Orvell Monitoring speichert alle PC- und Internet-Aktivitäten ähnlich einem Videorekorder.

Orvell Monitoring 2004 verfügt außerdem über einen leistungsstarken Keylogger zur **Aufnahme aller Tastenanschläge**. Auch Sondertasten, Tastenkombinationen und sogar die Zwischenablage wird aufgezeichnet.

Ein eingebauter **Internetrekorder** nimmt die Adressen der besuchten Webseiten (URLs) auf und der **Programmrekorder** registriert den Start von allen Programmen. Sie erfahren, welcher Benutzer wann welche Software gestartet hat und welche Internetseiten angesurft wurden.

Weitere Programme

NEUHEIT! Winston Monitoring: der Spezialist zur Überwachung per eMail.
Weitere Software zur PC- und Netzwerküberwachung
Welche Monitoringsoftware für welche Anwendung? Test & Vergleich

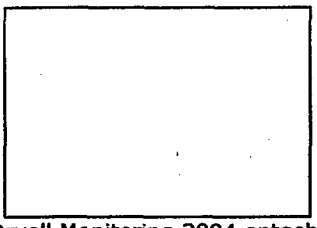
Service

- Sofort kaufen
- Telefonische Hotline
- Support/eMail
- Netzwerk
- Funktionsübersicht
- Produktbeschreibung (PDF; ca. 800 Kb)
- Newsletter
- Affiliate-Programm für Webmaster/Reseller

Einsatzbeispiele

- Was erlebt Ihr Kind oder Ihr Partner am PC?
- Erfahren Sie, wer Ihre Computer für welche Zwecke benutzt
- Visuelle Überwachung von Schul- und Firmennetzwerken (Rufschädigung, Wirtschaftsspionage...

In Verbindung mit der **Bildschirmaufnahme** erfahren Sie ebenfalls, welche eMail empfangen bzw. versendet wurde und welche Chat Unterhaltungen stattgefunden haben.



Orvell Monitoring 2004 entgeht nichts!

Automatische Aufnahme jeglicher PC Aktivitäten:

- alle besuchten Webseiten
- alle eMails und Chat-Unterhaltungen
- alle Tastenanschläge
- alle Bildschirmoberflächen (visuelle Überwachung)
- alle Dateiänderungen (neu)
- alle Anwendungen (auch PC-Spiele!)

Doch die Aufnahme aller Aktivitäten ist nicht alles...

Schlüsselworterkennung und eMail Reporte

Eine der Stärken von Orvell Monitoring ist die Schlüsselworterkennung und -benachrichtigung. Stellen Sie eine Liste von Wörtern oder Phrasen zusammen und Orvell Monitoring informiert Sie sofort, wenn eines dieser Wörter über die Tastatur eingegeben wurde oder in einer URL vorkommt. Sie definieren, bei welchen Schlüsselwort und Phrasen Orvell Monitoring reagieren soll. Zum Beispiel, "sex", "Telefonnummer", usw.

Sobald ein Schlüsselwort erkannt wird, erhöht Orvell Monitoring automatisch die Geschwindigkeit der Bildschirmaufnahmen. Es wird dann beispielsweise für die Dauer von 60 Sekunden alle 5 Sekunden (frei einstellbar) eine Bildschirmaufnahme getätigt. Somit erfahren Sie im Detail, was zu diesem Zeitpunkt passiert ist. Danach wird wieder mit der normalen Geschwindigkeit (z.B. alle 30 Sekunden) aufgenommen.

Weiter kann Orvell Monitoring so eingestellt werden, dass Sie bei dem auftauchen dieser Schlüsselworte SOFORT per eMail informiert werden. Orvell Monitoring sendet dann umgehend eine Benachrichtigung an Ihre eMail Adresse, sobald ein Schlüsselwort erkannt wurde. Jede Benachrichtigungsmail beinhaltet folgende Informationen: das erkannte Schlüsselwort, Datum/Uhrzeit, Ort (Tastatur, URL) und der zu dem Zeitpunkt der Erkennung angemeldete Windows Benutzer.

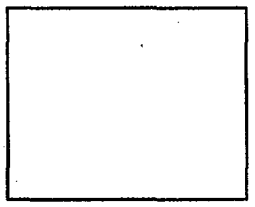
Somit wissen Sie sofort was passiert ist, damit Sie schnell handeln können.

Super Tarnfunktion

Die Tarnfunktion versteckt Orvell Monitoring vor jedem - außer Ihnen. Orvell Monitoring erscheint nicht in der System Tray, auf dem Desktop oder unter "Software" in der Systemsteuerung. Orvell Monitoring kann nur durch die Ihnen bekannte

Wirtschaftsspionage...
)

Aufforderung der Bundesfamilienministerin.



Funktionsumfang

- Automatische Aufname aller PC Aktivitäten
- Super Tarnmodus
- Aufnahme aller Bildschirmoberflächen
- Aufnahme aller besuchten Interentseiten (URLs)
- Aufnahme aller Tastenanschläge inklusive Tastenkombinationen!
- Aufnahme aller gestarteten Programme (NEU!)
- Aufruf über nur Ihnen bekannte Hotkeys
- Präzises User Tracking
- Aufnahme eines Netzwerks
- Start mit Windows
- Internet Online Update Funktion
- Bedienung wie an einem Videorekorder
- Passwort Schutz
- Textsuche
- Aufnahme/Export in schwarz/weiß oder Farbe
- Kompression
- Standby Modus
- Benutzerfreundliche Oberfläche
- Einfach zu benutzen. Sie benötigen keine Vorkenntnisse!
- und vieles mehr!

Monitoring Newsletter

eMail-Adresse

anmelden abmelden

Abschicken

Tastenkombination mit Ihrem Passwort aufgerufen werden. Nur Sie können Orvell Monitoring öffnen, die Aufzeichnungen ansehen bzw. löschen, Überwachungsänderungen tätigen oder deinstallieren.

Abschicken

Mit Orvell Monitoring verfügen Sie über eine professionelle und leistungsfähige Software zur Aufnahme aller Vorgänge an Ihrem Computer. Komplett in deutsch!

Klicken Sie hier, um Orvell Monitoring 2004 sofort herunterzuladen.

Funktionsübersicht | Screenshots | FAQ | Systemanforderungen

Hinweise

Bitte beachten Sie folgenden wichtigen Hinweis für den Einsatz in Deutschland: unsere Software verfügt über Überwachungsfunktionen (insbesondere "Tastaturmitschnitt" und "Bildschirmaufnahme"), die der Genehmigung der zu überwachenden Personen bedarf. Sie machen sich bei Nichtbeachtung im Sinne von §201, §202 StGB strafbar. Bei Verwendung der Software in anderen Ländern müssen Sie sich über die dortigen gesetzlichen Bestimmungen informieren und diese beachten.

Winston Monitoring 2004

PC Überwachungssoftware
Spezialisiert auf eMail Versand

Aufnahme aller PC Aktivitäten
- jeder Tastenanschlag & Anwendung
- jede Internetseite & PC Start
- Neuheit: Aufnahme über WebCam

Produktinformationen zu Winston

NEU! Winston Monitoring 2004 - Aufnahme aller PC Aktivitäten mit eMail Versand

Die PC Überwachungssoftware Winston Monitoring 2004 zeichnet unbemerkt im Hintergrund alle PC Aktivitäten auf und versendet regelmäßig detaillierte Berichte der PC Nutzung an Ihre eMail Adresse.

Winston wurde dazu entworfen, alle Computeraktivitäten automatisch aufzuzeichnen und zu speichern:

- **jede besuchte Internetseite**
- **jede gestartete Anwendung**
- **jeder Tastenanschlag**
- **jede geschriebene eMail**
- **jeder PC Start und vieles mehr!**

Neuheit: die Alarmfunktion reagiert auf verdächtige Aktivitäten und **fotografiert über eine Webcam den aktuellen Benutzer.** Sie erhalten das Bild sofort per eMail.
Mit Winston nehmen Sie alle Computeraktivitäten schnell und einfach auf - ausführlich bis zum letzten Tastenanschlag. Regelmäßig (z.B. alle 30 Minuten) und voll automatisch erhalten Sie die Aktivitätsreporte per eMail. Auf Wunsch völlig unsichtbar, ohne die Arbeit zu stören.
Weitere Informationen...

Wenn Ihnen Winston Monitoring 2004 gefällt, dann lesen Sie...
Orvell Monitoring funktioniert ähnlich Winston. Durch die zusätzliche visuelle Bildschirmaufnahme per Screenshots **sehen Sie**, was an andere Personen an Ihrem Computer erleben. Wie eine Überwachungskamera macht Orvell regelmäßig Aufnahmen des Bildschirms. Die Aufnahmen werden versteckt und komprimiert auf Ihrer Festplatte abgelegt.
Weitere Informationen zu Orvell Monitoring...

Produktservice

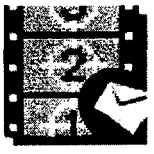
Unverbindliche Beratung per Telefonhotline (Montag-Freitag) oder per eMail.

Weitere Programme

Orvell: alle PC Aktivitäten visuell überwachen! Bis zum letzten Tastenanschlag...
Weitere Software zur PC- und Netzwerküberwachung
Welche Monitoringsoftware für welche Anwendung? Test & Vergleich

Service

- Telefonische Hotline
- Support/eMail
- Funktionsübersicht
- Winston im Netzwerk
- Newsletter
- Affiliate-Programm für Webmaster/Reseller



Aktuelle Umfrage

Die meisten Deutschen (56 Prozent) haben laut einer Umfrage Verständnis dafür, dass Unternehmen ihre Internetnutzung am Arbeitsplatz kontrollieren. Für die repräsentative EMNID-Umfrage im Auftrag der Programmzeitschrift "auf einen Blick" wurden 1000 Menschen ab 14 Jahren befragt. Hier das Ergebnis...

Funktionsumfang

- Automatische Aufnahme aller PC Aktivitäten

Aktivitäten

- Super Tarnmodus
- Aufnahme aller *besuchten* Internetseiten (URLs)
- Aufnahme aller gestarteten Programme
- Aufnahme aller Tastenanschläge
- Frei definierbare Schlüsselwortliste zur Erkennung verdächtiger *Aktivitäten*
- Alarmfunktion: sofortige Zusendung des Reportes
- **Neuheit:** Aufnahme des Benutzers über eine handelsübliche Webcam
- Aufruf über nur Ihnen bekannte Tastenkombinationen (Hotkeys)
- Passwortschutz
- Zusendung der Überwachungsreporte per eMail
- Automatische Deinstallation möglich
- Reporte in HTML/Text Format
- Versand/Empfang der Reporte über *Freemailer (web.de,* gmx.de, etc.) oder T-Online, etc. möglich
- und vieles mehr!
- Einfach zu benutzen. Sie benötigen keinerlei Vorkenntnisse

Monitoring Newsletter

eMail-Adresse

anmelden abmelden

Abschicken

Hinweise

Bitte beachten Sie folgenden wichtigen Hinweis für den Einsatz in Deutschland: unsere Software verfügt über Überwachungsfunktionen (insbesondere "Tastaturmitschnitt" und "Webcamaufnahme"), die der Genehmigung der zu überwachenden Personen bedarf. Sie machen

sich bei Nichtbeachtung im Sinne von §201, §202 StGB strafbar. Bei Verwendung der Software in anderen Ländern müssen Sie sich über die dortigen gesetzlichen Bestimmungen informieren und diese beachten.

Der Einsatz solcher Technologien erlaubt es dem Dienstgeber – eventuell dem Ressortchef oder leitendem Beamten – jede Aktivität der MitarbeiterInnen auf ihren EDV-Arbeitsplätzen zu kontrollieren. Jede besuchte Internetseite kann aufgezeichnet werden, jedes Email, das gesendet oder empfangen wurde, kann der Dienstgeber lesen, alle Tastenanschläge werden gespeichert, wann welches Programm aufgerufen wird wird dem Dienstgeber mitgeteilt und durch regelmäßige Bildschirmaufnahmen können alle Chatunterhaltungen und sonstige Anwendungen (auch Spiele) registriert werden.

Nicht umsonst wurde für ein Programm der Titel „Orvell Monitoring" gewählt: Alle DienstnehmerInnen werden für den Dienstgeber zur gläsernen Person.

Die unterzeichneten Bundesräte richten daher an das genannte Mitglied der Bundesregierung folgende

Anfrage

1. Haben Sie oder ihr Ressort Software beschafft, die es ermöglicht, das Verhalten der MitarbeiterInnen am EDV-Arbeitsplatz zu überwachen oder zu kontrollieren?

2. Wenn ja, um welche Software handelt es sich genau? Wieviele Lizenzen wurden angekauft?

3. Wenn ja, welche Kosten hat diese Beschaffung verursacht?

4. Wenn ja, wie wird diese Software im Detail eingesetzt? Welche MitarbeiterInnen werden in welchem Umfang überwacht?

5. Wenn ja, auf welcher Rechtsgrundlage basiert der Einsatz dieser „Überwachungs-Software"?

6. Wenn ja, haben sie diesen Einsatz mit der Personalvertretung abgesprochen?

7. Wenn ja, wurden von diesem Einsatz alle MitarbeiterInnen umfassend informiert?

8. Wenn ja, was passiert mit den aufgezeichneten Daten und wer hat Zugang aus welchen Gründen zu diesen?

9. Wenn ja, was soll mit der Überwachung erreicht werden?

10. Wenn ja, haben diese Überwachungen zu konkreten dienstrechtlichen Schritten gegenüber einem oder mehreren MitarbeiterInnen geführt?

11. Wenn gegenwärtig noch kein konkreter Einsatz dieser Software in ihrem Ressort erfolgt, gibt es Überlegungen, in Zukunft eine solche zu beschaffen? Wenn ja, aus welchen Gründen?