

*Machen Sie doch, was Sie wollen..
Wir helfen Ihnen dabei.*

Gerrit Wiegand, Jens Möisinger

Kontrollpotentiale bei elektronischer Kommunikation

Was Überwachungstechnik alles möglich macht
Anwendungsbeispiele aus der Praxis
Demonstration zum Thema
„Big Brother“ am Arbeitsplatz

am 11.05.2011 in Köln
im Rahmen der Veranstaltung
„SoliServ-Forum für Arbeitnehmervertreter - Arbeitsrecht und Datenschutz 2011“

Der User: Grünschnabel



IT-Service GmbH

Erich-Ollenhauer-Straße 24

63073 Offenbach

☎ 069 / 89009541

✉ gruenschnabel@mainis.de

Gregor Grünschnabel

Der Admin: Rothschild



IT-Service GmbH

Erich-Ollenhauer-Straße 24


63073 Offenbach

☎ 069 / 89009540

✉ rothschild@mainis.de

Robert Rothschild

08.11.2010 17:15

 « [Vorige](#) | [Nächste](#) »

Studie: Datenschutzverstöße in Betrieben sind keine Petitesse

 [verlesen](#) / [MP3-Download](#)

Zahlreiche Unternehmen missachten den Anspruch ihrer Beschäftigten auf Sicherung der Privatsphäre: Jeder siebte Betriebsrat berichtet von Verstößen gegen geltende gesetzliche Vorschriften. Das hat eine Studie (PDF-Datei) des Wirtschafts- und Sozialwissenschaftlichen Instituts (WSI) der Hans-Böckler-Stiftung herausgefunden. 14 Prozent der dafür knapp 2000 repräsentativ befragten Betriebsräte berichteten demnach über einen rechtswidrigen Umgang mit Informationen über die Arbeitnehmer. Die Dunkelziffer dürfte noch darüber liegen, erläutert Umfrageleiter Martin Behrens, da Betriebsräte nicht von jedem Fall erfahren würden. Kleine Firmen mit weniger als 20 Beschäftigten sowie Betriebe ohne Arbeitnehmervertretung seien zudem nicht erfasst worden.

Einblick in E-Mail, Kalender und Kontakte

Protokollierung im Internet

Fernzugriff auf den PC

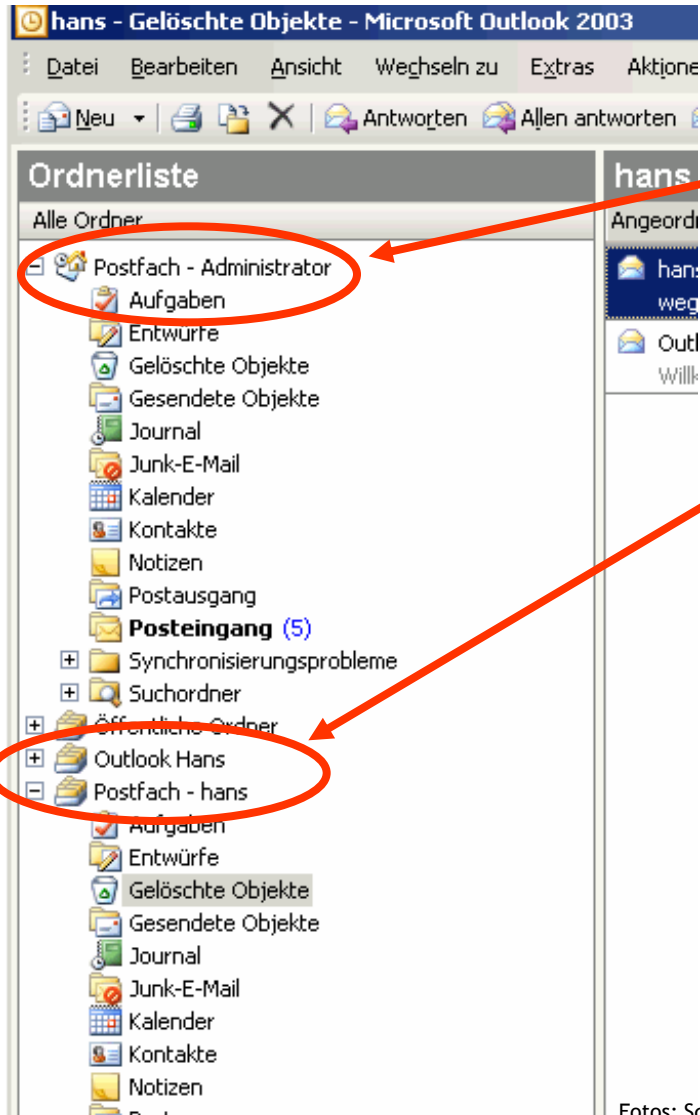
Überwachung von Mobilität / Handy

Telefon-Überwachung

Spionage-Software

- **Öffnen des Postfaches durch Administratoren**
 - Praktisch jedes E-Mail-Programm legt seine Daten in Dateien ab, die ohne großen Aufwand eingesehen werden können (bspw. über administrative Laufwerksverbindungen)
 - Auswertung des E-Mail-Verkehrs eines bestimmten PCs
 - Nur am Gerät selbst oder per Laufwerkszugriffe möglich und damit relativ aufwändig
 - Nur für Einzelfall-Kontrollen geeignet
 - Keine Restriktions-Möglichkeiten, nur Kontrolle

Lokale Überwachung von E-Mail-Aktivitäten: Postfach-Verbindung - Demo



Angemeldeter Benutzer

Verbundenes Postfach
von einem anderen
Benutzer

Fotos: Screenshot Microsoft Outlook 2003

- „Standardmäßige“ Überwachungsmöglichkeiten des E-Mail-Verkehrs durch Protokolle:
 - Jeder E-Mail-Server (bspw. Exchange, Lotus Domino) schreibt Protokolle über die versendeten E-Mails
 - Jede Mail ist bis zum endgültigen Versand durch den Server im Klartext lesbar
 - Protokolle sind nötig zum Betrieb des Netzwerks, aber:
 - Oft sind sie gar nicht bekannt
 - Meist sind sie nicht abschaltbar
 - Oft ist die Aufbewahrungsdauer und Löschung nicht geregelt

Zentrale Überwachung von E-Mail-Aktivitäten: Protokolle: Beispiel Exchange

Timestamp	MessageSubject	Sender	Recipients
2010/11/04 09:56:32	< Zugesagt: Big Brother 2.0 Generalprobe	demeter@m[REDACTED]	moesinger@m[REDACTED]
2010/11/04 09:57:21	< Patrick	patrickr9@w[REDACTED]	info@m[REDACTED]
2010/11/04 09:57:22	< Backup Exec-Meldung: Medium einlegen	mainis@fin[REDACTED]	betreuung@m[REDACTED]
2010/11/04 09:57:23	< Gateway IP Monitor: Current IP address i	administrator@herrm	betreuung@m[REDACTED]
2010/11/04 09:57:24	< Gateway IP Monitor: Current IP address i	administrator@herrm	betreuung@m[REDACTED]
2010/11/04 09:57:26	< Bis zu 100€ für Neukunden zb. für Hanno	team@m[REDACTED]	websupport@m[REDACTED]
2010/11/04 10:03:31	< Windows Small Business Server 2008: B	SBSMonAcct@innov	betreuung@m[REDACTED]
2010/11/04 10:03:32	< Windows Small Business Server 2008: B	SBSMonAcct@schoe	betreuung@m[REDACTED]
2010/11/04 10:03:33	< Nur jetzt - shoppen als VIP	charles-voegele@ne	websupport@m[REDACTED]
2010/11/04 10:09:30	< Re: AW: AW: Weihnachtsfeier und so die	polyhymnia-bieber@	arnold@m[REDACTED]
2010/11/04 10:09:31	< Backup Exec-Meldung: Medium einlegen	backup-admin@proje	betreuung@m[REDACTED]
2010/11/04 10:12:29	< Eilmitteilung zur Kreditvergabe	newsletter@b2cmail8	demeter@m[REDACTED]
2010/11/04 10:12:30	< Gateway IP Monitor: Current IP address i	administrator@schin	betreuung@m[REDACTED]
2010/11/04 10:12:31	< Gateway IP Monitor: Current IP address i	administrator@schin	betreuung@m[REDACTED]
2010/11/04 10:12:32	< Backup Exec-Meldung: Medium einlegen	mainis@fin[REDACTED]	betreuung@m[REDACTED]
2010/11/04 10:14:53	< Zugesagt: Big Brother 2.0 Generalprobe	scherf@m[REDACTED]	moesinger@m[REDACTED]

Zeitpunkt

Betreff

Absender

Empfänger

Zentrale Überwachung von E-Mail-Aktivitäten: Filter

- **Virens Scanner oder Spam-Filter**

- Sie „lesen“ jede E-Mail, um schadhafte Routinen oder Werbung zu erkennen und zu entfernen
- Dazu ist die Analyse des **Inhalts** (Worte, Zeichen, Bilder etc.) notwendig
- Die meisten Filter protokollieren ihr Vorgehen

- **E-Mail-Filter**

- Sie „lesen“ jede E-Mail, um Regeln darauf anzuwenden:
 - Vorsortierung
 - Restriktionen (z.B. gesperrte Empfänger)
 - Alarmierungen (z.B. Benachrichtigung von Vorgesetzten)
- Sie „verstehen“ Mails inhaltlich
- Sie haben umfangreiche Protokollierungen/Auswertungen

Erkennungsmechanismen von Filtersoftware: Google-Mail

★ **Google Video** an mich [Details anzeigen](#) 7. Mai. (vor 2 Tagen) [Antworten](#)

Anzeigen

Sehr geehrter Google Videos-Nutzer,

wir haben Ihnen in der vergangenen Woche eine E-Mail gesendet, in der wir Ihnen mitgeteilt haben, dass wir ab dem 29. April keine Videos mehr auf Google Videos abspielen können. Wir haben Ihnen ferner Anleitungen gegeben, wie Videos herunterzuladen sind, die derzeit auf der Plattform gehostet werden. Seit diesem Zeitpunkt haben wir von Ihnen Feedback dazu erhalten, wie die Migration von Google Videos vereinfacht werden kann. Wir arbeiten täglich daran, Ihnen eine positive Nutzererfahrung zu bieten, und versuchen uns da zu verbessern, wo wir hätten besser sein können. Auf der Grundlage Ihres Feedbacks arbeiten wir zwecks Verbesserungen an Folgendem:

Wir versichern Google Videos-Nutzern, dass sie keine ihrer Inhalte verlieren werden und streichen den Stichtag am 29. April. Wir arbeiten daran, Ihre Google Videos automatisch zu YouTube zu migrieren. In der Zwischenzeit bleiben sowohl Ihre auf Google Videos gehosteten Videos im Web als auch alle bestehenden Links zu Google Videos zugänglich. Sie möchten jetzt nach YouTube migrieren? So funktioniert's:

Wir haben auf der [Statusseite](#) von Google Videos die Option "Videos auf YouTube hochladen" hinzugefügt.

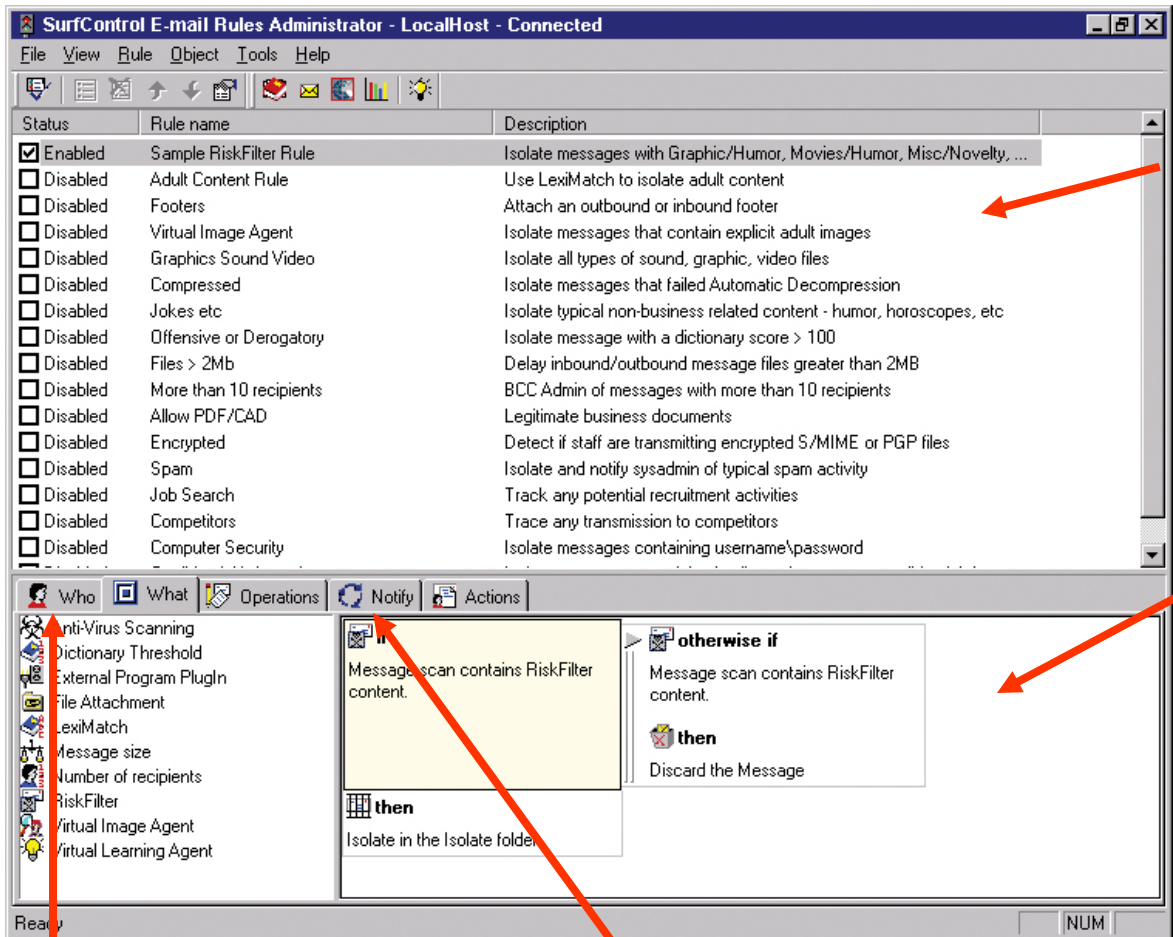
Urheberrecht, Wettbewerb
Ihr Spezialist in
Frankfurt am Main
www.fortmeyer.de

Seminare Musikmanagement
Fit im Musikbusiness, für Ihren Job
bei Labels, Verlagen & Veranstaltern
www.akademieeins.com

Ihre Online-Festplatte
Ihre Dateien online anzeigen und
weitergeben - direkt im Browser.
www.filespots.de

Weitere Informationen zu
[Youtube Video »](#)
[Videos Hochladen »](#)
[You Tube Youtube »](#)
[Youtube FLV »](#)

Zentrale Überwachung von E-Mail-Aktivitäten: Filter: Beispiel SurfControl



Liste der Ereignisse, z.B.

- „Adult Content Rule“
- „Image Agent“
- „Encrypted“

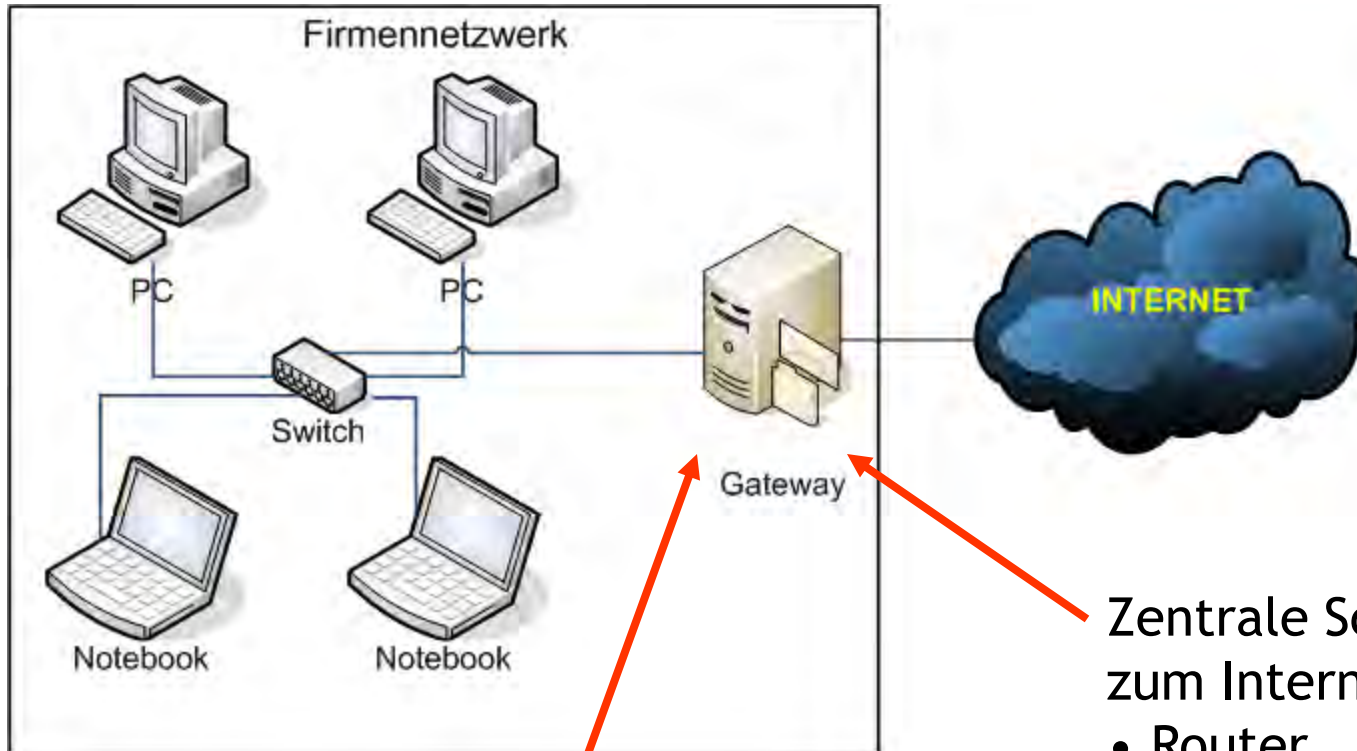
Verfahrensanweisungen beim Zutreffen einer Regel, z.B.

- „Löschen“
- „Zurückschicken“
- „Zwischenspeichern“

Benutzerabhängige
Regeln

Automatische
Benachrichtigungen

Zentrale Überwachung von Internet-Aktivitäten: Aufbau



Zentrale Schnittstelle zum Internet, bspw.

- Router
- Firewall
- Proxy-Server

Geeigneter Angriffspunkt für „Lausch-Software“, aber auch oft Datenpool von Standard-Protokollen (z.B. MS-Exchange, Lotus Domino etc.)

Zentrale Überwachung von Internet-Aktivitäten

- **Zentrale Überwachung bedeutet:**
 - Die Daten werden an einem zentralen Punkt gesammelt (dem „Internet-Gateway“)
 - Unabhängig vom einzelnen Arbeitsplatzrechner
 - Für zentrale Auswertungen und auch für präventive Überwachungen/Restriktionen einsetzbar
 - Protokolle sind nötig zum Betrieb des Netzwerks, aber:
 - Oft sind sie gar nicht bekannt
 - Meist sind sie nicht abschaltbar
 - Oft ist die Aufbewahrungsdauern und Löschung nicht geregelt

Proxy-Server

- Proxy-Server vermitteln Anfragen an das Internet aus dem Unternehmens-Netzwerk an das Internet weiter („routing“)
 - Da jeder einzelne Internet-Aufruf an dieses Programm weitergegeben wird, liegt es nahe, diese Aufrufe auch zu protokollieren
 - Die Protokolle werden faktisch immer geschrieben, auch wenn sie gar nicht ausgewertet werden
 - Der Datenpool ist hochgradig brisant, da entsprechende Auswertungsprogramme beliebige Statistiken erstellen können (benutzerabhängige Zugriffe, Zugriffe auf einzelne Seiten etc.)
- Sie können auch zur Sperrung/Beschränkung von Benutzern oder Seiten eingesetzt werden
- Gleiches geht auch mit Firewalls, Routern u.a.

Zentrale Überwachung von Internet-Aktivitäten: Proxy-Server - Demo



GFI WebMonitor for ISA Server



GFI WebMonitor | GFI MailEssentials | GFI MailSecurity | GFI DownloadSecurity | GFI LANguard

Refresh Support Reset data Data collected from: 17:48 24/9/2004

Web access in progress	URL history	Users history	Last web access	Configuration
URL:	Hits:	Real filetypes:	#	Users or IP if not authen.(hits):
www.verdi.de	89	html:5	1	frater-magnus\gerrit(89)
www.msn.de	57	html:4 jpg:15 gif:35	1	frater-magnus\gerrit(57)
www.realvnc.com	15	html:3 jpg:3 gif:6 executable:1	1	frater-magnus\administrator(15)
.com	10	html:10	2	frater-magnus\5) 127.0.0.1(5)
www.verdi-bildungsportal.de	2		1	frater-magnus\gerrit(2)
www.macromedia.com	2		1	frater-magnus\gerrit(2)
www.adobe.de	2		1	frater-magnus\gerrit(2)
magnus.frater-magnus.local	1	html:1	1	frater-magnus\administrator(1)
www.google.de	2	html:1 gif:1	1	frater-magnus\gerrit(2)
www.microsoft.com	1	html:1	1	frater-magnus\gerrit(1)
emealqin.msn.com	1	html:1	1	frater-magnus\gerrit(1)
msid.eu.msn.com	1	html:1	1	frater-magnus\gerrit(1)
a.tfaq.de	4	html:1 gif:1	1	frater-magnus\gerrit(4)
msn.ivwbox.de	2	gif:1	1	frater-magnus\gerrit(2)
c.msn.de	1	gif:1	1	frater-magnus\gerrit(1)
ad.de.doubleclick.net	3	html:1 flash:1	1	frater-magnus\gerrit(3)
www.passportimages.com	1	gif:1	1	frater-magnus\gerrit(1)
global.msads.net	1	gif:1	1	frater-magnus\gerrit(1)

Aufgerufene
Seiten,
hier:

- ver.di
- Adobe
- Google

Anzahl Aufrufe
pro Benutzer

Benutzername

Fotos: Screenshot GFIWebMonitor (www.gfi.com)

- Grundsätzlich ähnliche Technik wie Proxy-Server u.ä., aber viel komfortablere Auswertungs-, Restriktions- und Alarmfunktionen:
 - Zeit- oder Volumenbegrenzungen für Benutzer
 - Sperrung bestimmter Seiten
 - Alarmfunktionen beim Aufruf „unliebsamer“ Seiten
 - Überwachen meist mehrere Internet-Anwendungen gleichzeitig (nicht nur WWW, sondern auch Chat, FTP, E-Mail etc.) und stellen somit noch umfangreichere Daten zur Verfügung

Zentrale Überwachung von Internet-Aktivitäten: Filter-Software - Demo

The screenshot shows the SurfControl Monitor application window. It has a menu bar (File, View, Configure, Window, Help) and a toolbar with various icons. The main area is divided into two panes: 'Sites' and 'Users'. Both panes have a search field and a table of data.

Sites Table:

Host Name	IP Address	First Seen	Last Seen	Hits	Category
www.winmaniabbs.net	0.0.0.0	2/9/01 2:15:02 PM	2/9/01 4:40:56 PM	11	Computing & Internet
ad.doubleclick.net	0.0.0.0	2/8/01 1:11:16 AM	2/12/01 4:34:13 PM	10	Advertisements
www.playboy.com	0.0.0.0	2/7/01 11:40:42 AM	2/10/01 10:36:27 ...	10	Adult / Sexually Explicit
www.proload.com	0.0.0.0	2/8/01 6:33:44 PM	2/9/01 3:00:58 AM	10	Weapons
www.interliant.com	0.0.0.0	2/13/01 7:08:32 PM	2/14/01 3:07:47 AM	10	None
cigarempire.com	0.0.0.0	2/10/01 9:58:28 AM	2/10/01 10:51:35 ...	10	Drugs & Alcohol
www.barleyhouse.com	0.0.0.0	2/11/01 12:53:46 ...	2/11/01 2:39:02 AM	9	Food & Drink
www.soccer.com	0.0.0.0	2/8/01 9:43:56 AM	2/11/01 9:52:46 AM	9	Sport
44logo.com	0.0.0.0	2/9/01 2:59:25 AM	2/9/01 3:31:09 AM	9	None

Users Table:

User Name	Workstation Name	IP Address	First Seen	Last Seen	Hits	Group
SMTP_Mail_Source	SMTP Mail Source	0.0.0.0	2/6/01 9:22:53 AM	2/8/01 5:41:16 PM	26	Mail Server
QACOM1\tim	timpc.sample.com	0.0.0.0	2/7/01 10:35:17 AM	2/10/01 12:59:36 PM	298	HR & RCP
QACOM1\roger	togerpc.sample.com	0.0.0.0	2/6/01 1:45:27 PM	2/9/01 6:12:05 AM	343	Admin
QACOM1\mark	markpc.sample.com	0.0.0.0	2/7/01 9:24:47 AM	2/11/01 11:42:03 PM	608	Tech Support
QACOM1\gareth	garethpc.sample.com	0.0.0.0	2/6/01 9:29:11 AM	2/9/01 4:27:52 PM	517	Sales
QACOM1\fred	fredpc.sample.com	0.0.0.0	2/6/01 9:24:35 AM	2/14/01 3:07:47 AM	168	Accounts
QACOM1\dave	davepc.sample.com	0.0.0.0	2/7/01 10:31:01 AM	2/13/01 5:26:41 AM	450	Tech Support
QACOM1\daniel	danielpc.sample.com	0.0.0.0	2/7/01 5:05:33 PM	2/10/01 8:33:35 PM	197	Development
QACOM1\claire	clairepc.sample.com	0.0.0.0	2/6/01 10:32:04 AM	2/9/01 11:50:48 PM	219	HR & RCP

At the bottom of the window, it says 'For Help, press F1' and '154 Records'.

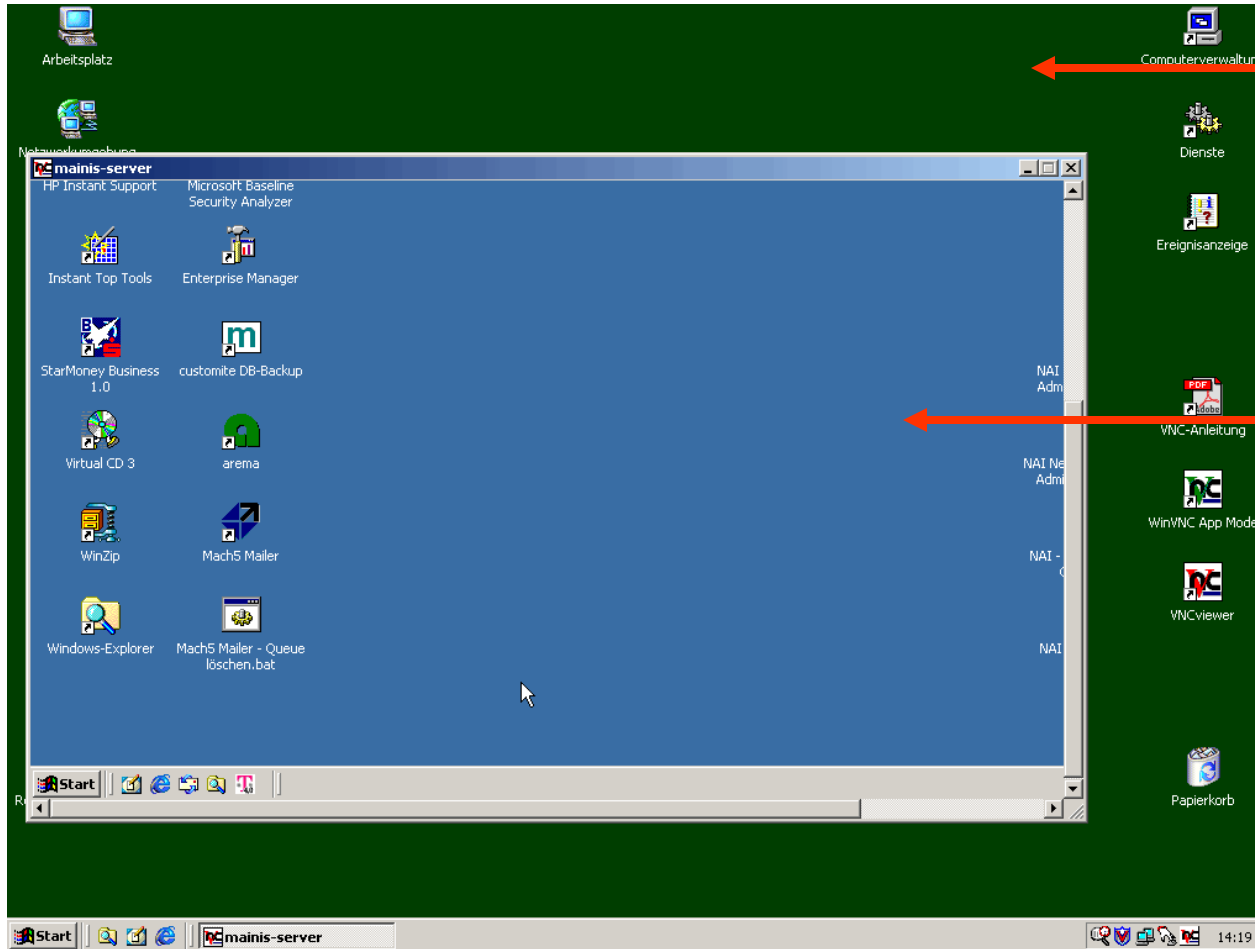
Auswahl
nach
Seiten

Auswahl
nach
Benutzern

- Der „Desktop“ ist die Benutzeroberfläche des Betriebssystems
- Verschiedene Kategorien der Überwachung:
 - Fernwartungs-Zugriffe für Echtzeit-Kontrollen
 - Administrative Laufwerkszugriffe
 - Diagnose- / Managementsoftware
 - Key-Logger (Hard- oder Software)
 - Spionage-Software
 - Für lokale Rechner
 - Im Netzwerk

- Die Technik ist eigentlich dazu gedacht, dem Benutzer bessere und schnellere Unterstützung zukommen zu lassen:
 - Der Fernwartungs-Zugriff ermöglicht es, den „Bildschirm“ des Benutzers auf einen anderen PC umzulenken und seine Arbeit zu beobachten oder zu beeinflussen
 - Es gibt i.d.R. verschiedene Modi des Zugriffs:
 - Der Benutzer wird vorher gefragt, ob er zustimmt
 - Die Verbindung ist für den Benutzer unsichtbar
 - Der Administrator beobachtet nur
 - Der Administrator greift ein, bspw. durch Mausbewegungen
 - Da Fernwartung nur in „Echtzeit“ möglich ist, eignet sie sich nur für eine gezielte und temporäre Kontrolle

Überwachung des Desktop: Fernwartungs-Zugriffe - Demo

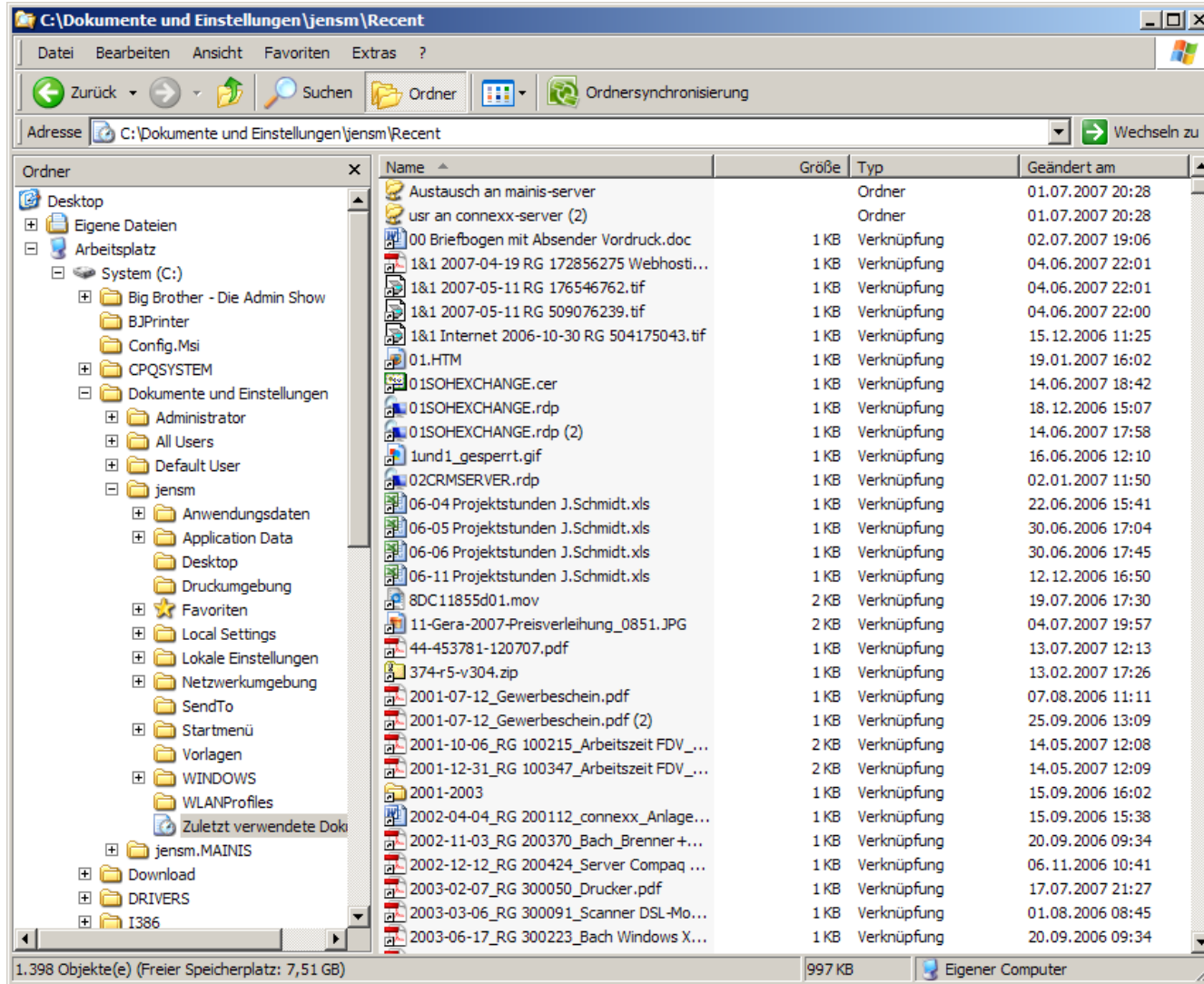


Rechner des
Administrators

Per Fernwartung
überwachter
Rechner des
Benutzers

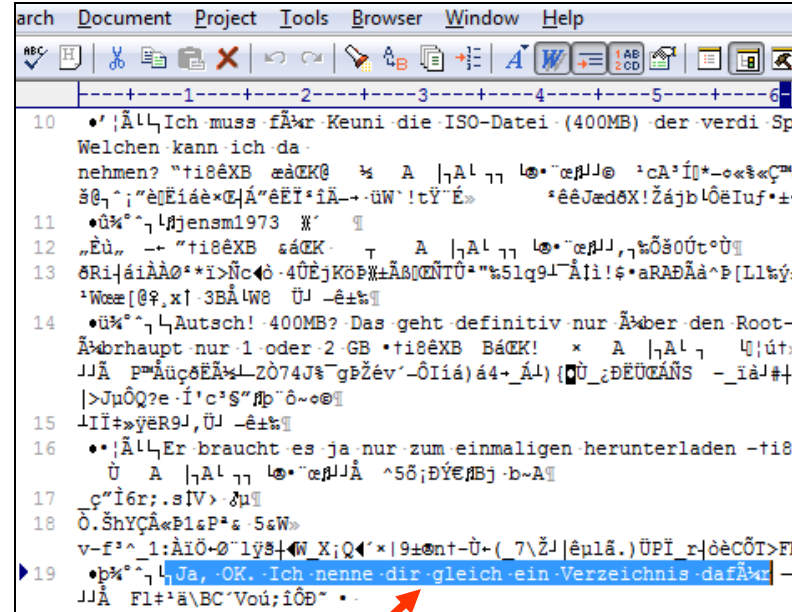
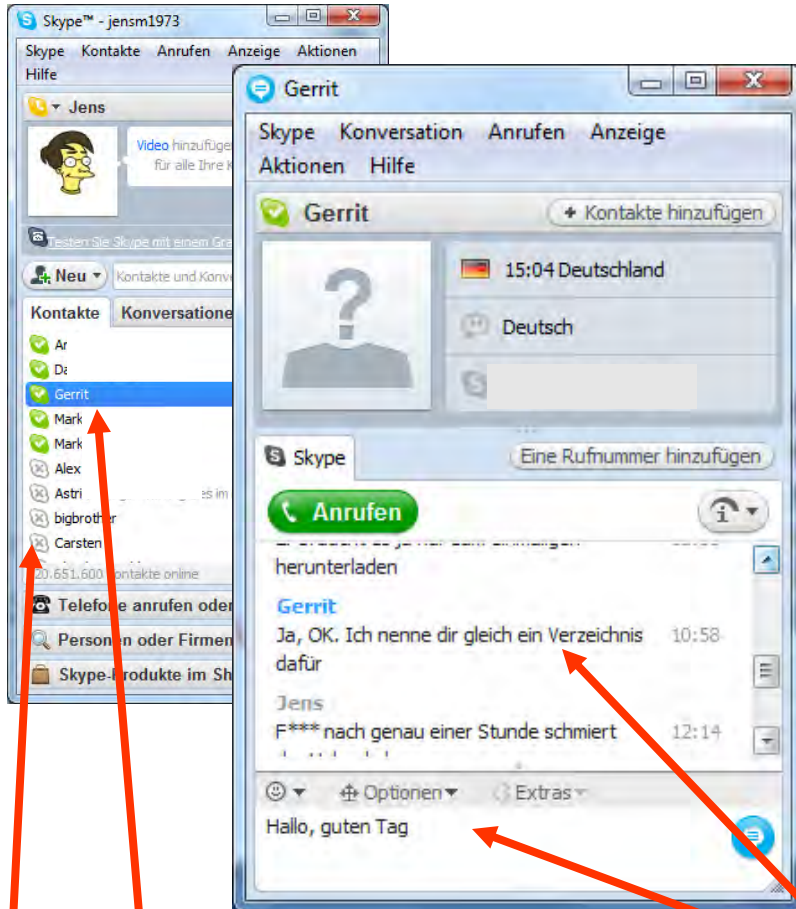
- In Netzwerken ist es möglich, dass sich Administratoren auf die Festplatten aller angeschlossenen PCs verbinden.
- Das ist nötig, um Software aus der Ferne zu installieren (z.B. Viren-Scanner-Updates), ohne Benutzer mit einbeziehen zu müssen.
- Über diese Freigabe sieht der Administrator alles, was lokal auf der Festplatte gespeichert ist - auch Protokolle und Einstellungen von Programmen, z.B.:
 - Zuletzt verwendete Dateien
 - Lokale Protokolle
 - Lokal gespeicherte Dateien

Überwachung des Desktop: Zuletzt verwendete Dateien- Demo



Fotos: Screenshot Microsoft Windows XP Pro

Überwachung des Desktop: Skype - Demo



entsprechender Text in Protokoll

Skype-Benutzer

Chatverlauf

Online-Status

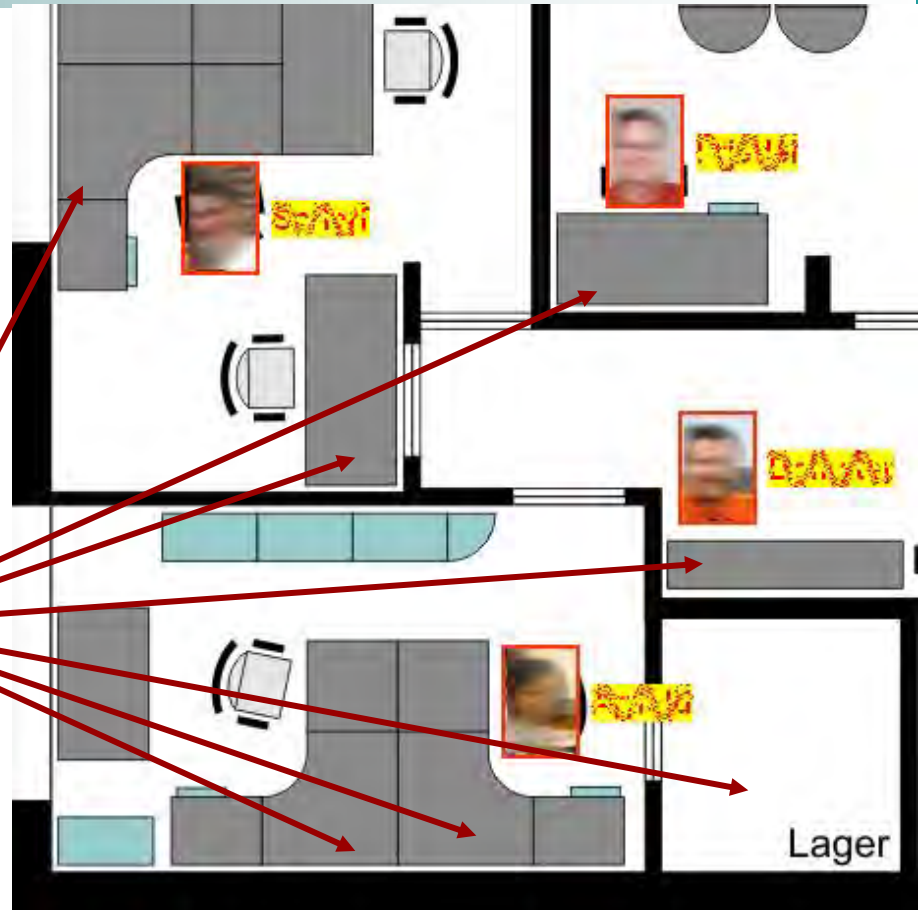
- RFID (Radio-Frequency Identification) bezeichnet eine Technik zum berührungslosen Auslesen von „Tags“, z.B. in Ausweisen, Schlüsseln, Kleidung etc.
- Jedes Tag hat eine eindeutige Nummer. Diese (und eventuell andere Daten) sendet es unbemerkt und vollautomatisch, wenn ein Lesegerät in der Nähe ist.
- Über die eindeutige Nummer lassen sich Aktionen auslösen:
 - Zeiterfassung (durch Mitarbeiterausweise)
 - Türen Öffnen (durch Schlüssel mit Tags)
 - Waren identifizieren und verteilen (durch Etiketten)
- Viele Tags brauchen keine Stromversorgung und sind damit sehr klein und günstig (ab ca. 0,05€)
- Leseabstand: Je nach Art bis zu mehreren Metern

Überwachung von Bewegung: RFID - Demo

MA-Ausweis mit
Tag (unsichtbar)



Berührungsfreie
Übertragung



RFID-Lesegeräte an
wichtigen Stellen

Überwachung von Bewegung: RFID in Textilien



mainis Artikel-Erkennung

Artikel-Erkennung

Artikel:	Sakko
Artikelnr.:	1258729
Artikel-ID:	0262015605404
Kunde:	236586
Verkaufsdatum:	07.03.11
Zahlung:	Kreditkarte
Weitere Käufe:	4
Umsatz 12 Mon.:	1.278,80 €
Bestkunde:	nein



Artikel erkannt! **Zeit: 10:21 Uhr**

Durch die eindeutige
Kennung:
Zusammenführung
mit Daten des
Zahlungsprozesses
möglich

Überwachung von Bewegung RFID - Beispiele

RFID in der Bekleidung

DTB informiert über Status Quo

Ende Juli lud der Dialog Textil Bekleidung zum RFID Paxistag nach Nußloch. Rund 70 Teilnehmer aus Industrie und Handel informierten sich über Anwendungsszenarien und Prozessoptimierungsmöglichkeiten.

RFID ist in der Bekleidung angekommen, lautete das Fazit der Veranstaltung, die mit zahlreichen Beispielen auf Handels- und Industrieseite und einer Live Demonstration im Betty Barclay Showroom RFID in der textilen Supply Chain anschaulich machte. Besonders die Erfahrungsberichte von Simon Essmeyer, George Gina & Lucy und Patric Knoll, Modehaus Jost, zeigten, wie der projektbezogene Einsatz von RFID auch ohne Einbeziehung der gesamten textilen Kette bereits respektable Ergebnisse erzielt. Auch wenn RFID laut Einschätzung von Robert Paulus, RF-iT Solutions und Ralf V. Bigge, GS1, zuerst bei vertikalen Bekleidungsanbietern zum Einsatz kommen wird – und das recht kurzfristig – so wurde dennoch klar, dass Unternehmen sich auch jetzt schon Wettbewerbsvorteile sichern können und mögliche Einsparungen wie auch prozessoptimierende Faktoren durch den Einsatz der Technologie bereits jetzt prüfen sollten.



RFID Live-Präsentation

Die Vision ist klar. Dass RFID bereits heute unternehmensübergreifend eingesetzt werden kann, in jedem Markt Tags problemlos verfügbar sind und notwendige Daten sicher ausgetauscht werden können, demonstrierten Heinz-Erich Ohnezat von Pranke, Heiko Tiedmann, Avery Dennison und Johannes Schick von der Firma Holtl. Zurzeit werden RFID Etiketten in der Regel beim Verkauf von Ware an Endverbraucher entfernt oder zerstört. Doch auch über den POS hinaus bestehen Nutzungs-

möglichkeiten, z.B. bei Reklamationen oder Pflegehinweisen. Verbrauchern muß halt die Wahl gelassen werden den Chip auch deaktivieren zu können. Deshalb sehen die Technologieanbieter den in den vergangenen Jahren immer wieder von Verbraucherschützern geäußerten Bedenken äußerst gelassen entgegen. Besonders großes Potential wird der RFID Technologie beim Einsatz als Warensicherung zugeschrieben, einem der bedeutenden Kostenfaktoren des Einzelhandels. Und wenn Bekleidungshersteller dank genauerer Bestandsinformationen besser, schneller und richtiger liefern, lässt sich mit RFID auch zusätzlicher Umsatz generieren.

www.dialog-dtb.de



von links: Anna Neuß, DTB; Oliver Stolbrock, RF; Patric Knoll, Modehaus Jost; Robert Paulus, RF-iT Solutions; und Simon Essmeyer, George Gina & Lucy

heise online

Home Newsticker 7-Tage-News N

heise online > News > 2010 > KW 9 > Mode

02.03.2010 18:21

Mode mit Funk

vorlesen / MP3-Download

Der Bekleidungsanbieter Gerry Weber ze seine anlaufende Routine-Handhabung R Unternehmen mit Hilfe des Infrastruktur-A auf die Logistik und Diebstahl-Vorbeugung waschbare, also recht langlebige Transpo Kleidungsstücke eingenäht. Diese Labels Ausland produzierten Waren auf dem We verfolgen. Außerdem sollen sie im Laden Ware das Weite sucht, ohne vorher bezah

Überwachung von Bewegung: RFID-Überwachung bei Veranstaltungen

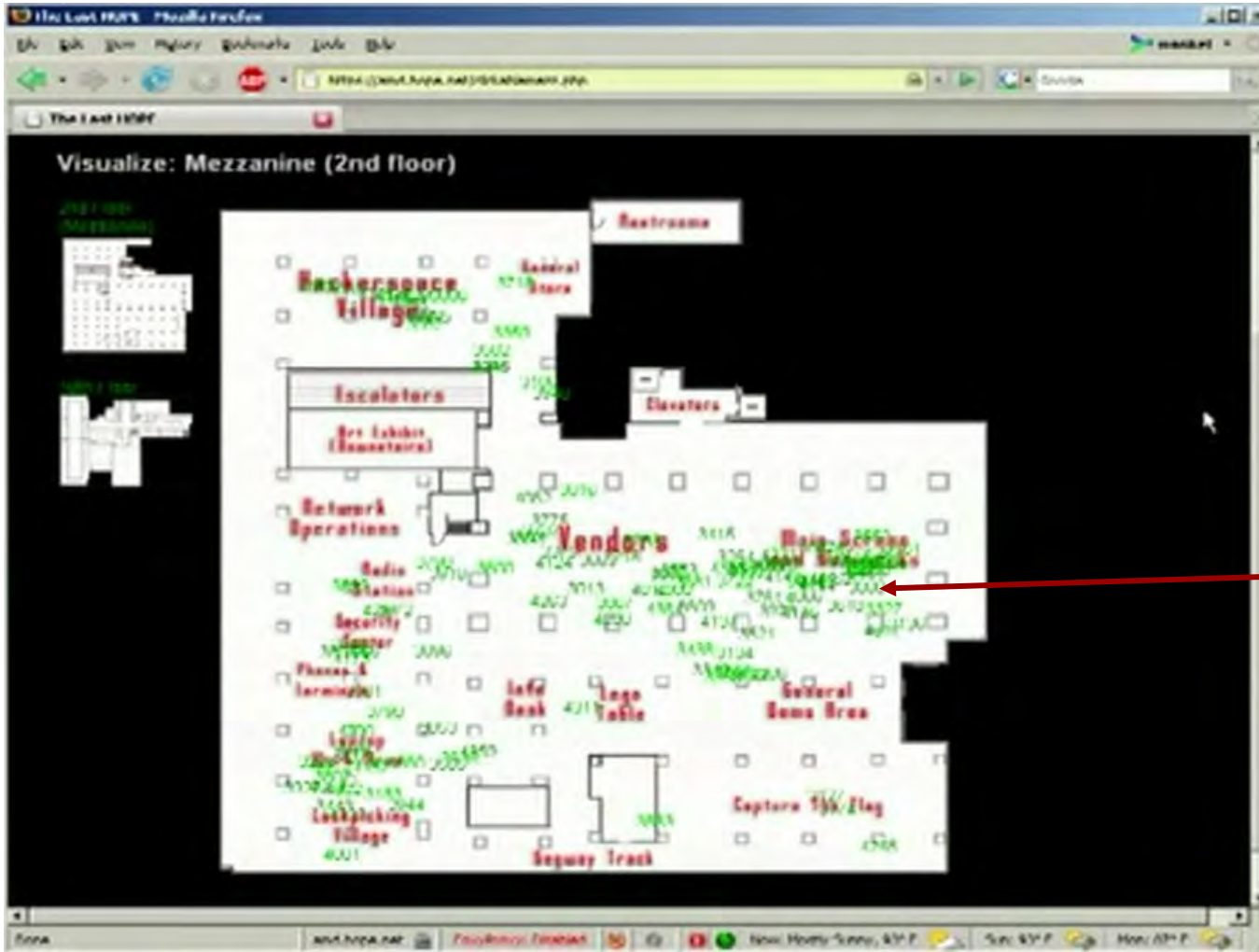


Abbildung eines Veranstaltungsraums der Konferenz „The Last Hope“ in 2008.

Jeder grüne Punkt ist ein (identifizierbarer) Mensch.

Genauigkeit:
ca. 0,2m

- Software zum Fernsteuern von Handys
 - Es wird eine SMS an das Handy geschickt, die eine spezielle Zeichenfolge enthält.
 - Diese SMS wird von der Software auf dem Handy entgegen genommen und die gewünschte Aktion ausgeführt:
 - Senden der Anruferliste per SMS oder E-Mail
 - Einschalten des GPS-Empfängers und senden der Position
 - Rückruf mit Lautsprech-Funktion (Babyfon) zur Spionage
 - Kopie des Adressbuchs versenden
 - Handy sperren/löschen/zurücksetzen
 - Der Zugriff ist i.d.R. unsichtbar und nur über evtl. Kosten (Einzelverbindungs nachweis) erkennbar
 - Oft entwickelt gegen Diebstahl (Wiederfinden, Sperren)

Überwachung von Bewegung: Handy auslesen - Demo



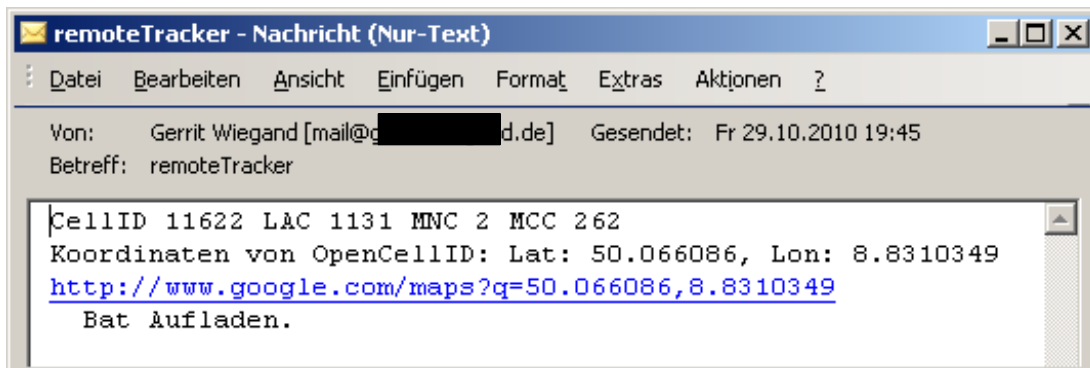
SMS mit speziellem Befehl,
z.B. rt#gp für GPS-Koordinaten

Rücksendung der gewünschten
Daten (z.B. Position,
Adressbuch, Anruferliste) als
SMS oder E-Mail)



Handy mit
Entsprechender
Software, z.B.
„RemoteTracker“.

Empfängt die SMS,
führt den Befehl
aus, löscht die SMS.



Beispiel-E-Mail mit
Positionsdaten und Link
auf Google-Maps

Überwachung von Bewegung: Das iPhone

SPIEGEL ONLINE

26. April 2011, 11:14 Uhr

Apple in der Kritik

iPhone ortet i

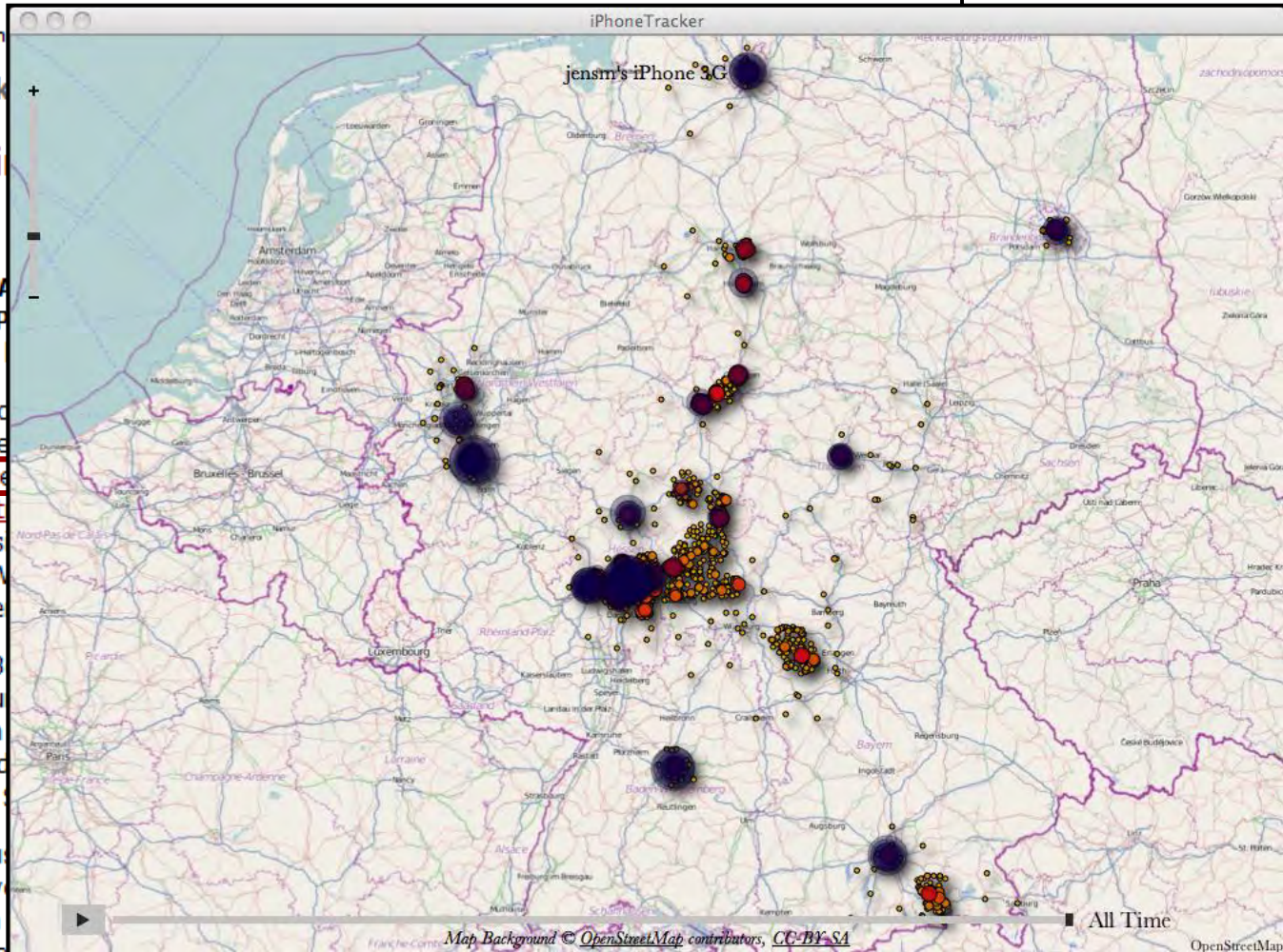
Von Ole Reißmann

Die Datenaffäre bei Apple zeigt, sammelt das iPhone Standortdaten, die die Funktion deaktiviert

Hamburg - Es lässt sich zeigen, dass Apple Nutzer und Telefon geortet. In den Einstellungen des Telefons kann man unter anderem das "Wall Street Journal" Software zur Beweissicherung bereits vergangene Wochen die Speicherung der Daten

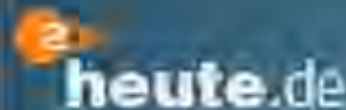
Hintergrund: In den bestimmten Anwendungen. Außerdem lassen sich herausstellen, hindert das daran, weiterhin den

Die Ortungsdaten, aus denen das iPhone dabei unweigerlich werden die sensiblen Daten 2010, als das aktuelle Betriebssystem eingeführt wurde, können die Daten zurückreichen.



Überwachung von Bewegung: Technische Entwicklungen

Wenn das Handy zum Big Brother wird



Japan: Arbeitnehmer sollen
mit Handy-Sensoren
überwacht werden

von Alfred Krüger

[...]

Der japanische Telekom-Konzern KDDI hat nun entdeckt, dass Beschleunigungssensoren auch für ganz andere Zwecke einzusetzen sind. In Unternehmen ermöglichen sie die lückenlose Überwachung der Mitarbeiter. Der Konzern hat nämlich eine Technologie entwickelt, die die Daten der Sensoren mit hoher Präzision analysiert. Dadurch lasse sich bestimmen, was eine Person, die ein entsprechendes Handy bei sich trägt, gerade macht: Ob sie gerade geht oder läuft, eine Treppe hochsteigt oder welche Arbeit sie gerade verrichtet.

Die Bewegungsdaten werden von den Beschleunigungssensoren aufgezeichnet und an einen zentralen Rechner geschickt. Hier werden die Daten ausgewertet und bestimmten Tätigkeiten zugeordnet. Dadurch lässt sich dann zum Beispiel zweifelsfrei ermitteln, ob eine Reinigungskraft auch wirklich den Boden wischt, fleißig Fenster putzt, Papierkörbe entleert oder gerade eine Zigarettenpause macht.

[...]

<http://www.heute.de/ZDFheute/inhalt/26/0,3672,8058234,00.html>

Überwachung von Bewegung: BlackBerry Server - Protokoll

```
PhoneCallLog_20090806.CSV - Editor
Datei Bearbeiten Format Ansicht ?
[Name.ID", "Type of Call", "Name", "Phone Number", "Start Date", "Server Log Date", "Elapsed Time", "Memo", "Command", "UID"
"Mark M [REDACTED].5", "Outgoing", "A [REDACTED]", "+49-0163-[REDACTED]", "2009/08/06 07:21:40", "2009/08/06
09:23:54", "00:00:00", "", "Add", "[REDACTED]8"
"Mark M [REDACTED].5", "Outgoing", "", "+49 (0) 69 - [REDACTED]", "2009/08/06 07:23:23", "2009/08/06
09:25:14", "00:00:00", "", "Add", "1974342211"
"Mark M [REDACTED].5", "Outgoing", "Herr M [REDACTED]", "69 [REDACTED]", "2009/08/06 07:23:56", "2009/08/06
09:25:15", "00:00:00", "", "Add", "1974342214"
"Mark M [REDACTED].5", "Outgoing", "Herr M [REDACTED]", "69 [REDACTED]", "2009/08/06 07:24:18", "2009/08/06
09:27:42", "00:01:58", "", "Add", "1974342216"
"Michael [REDACTED].12", "Outgoing", "M [REDACTED]", "+49 (151) [REDACTED]", "2009/08/06 10:35:44", "2009/08/06
12:45:45", "00:00:03", "", "Add", "556605562"
"Michael [REDACTED].12", "Incoming - Completed", "Mark [REDACTED]", "+49 (151) [REDACTED]", "2009/08/06 10:39:27",
12:45:46", "00:05:29", "", "Add", "556605564"
"Mark M [REDACTED].5", "Outgoing", "[REDACTED]", "016 [REDACTED]", "2009/08/06 11:14:11", "2009/08/06
13:16:10", "00:00:29", "", "Add", "1974342222"
"Michael [REDACTED].12", "Outgoing", "Sebastian [REDACTED]", "+49 (160 [REDACTED]", "2009/08/06 13:35:07", "2009/08/
15:35:54", "00:00:00", "", "Add", "55660 [REDACTED]98"
"Mark M [REDACTED].5", "Incoming - Missed Call, unopened", "[REDACTED]", "017 [REDACTED]", "2009/08/06 14:24:18",
16:25:27", "00:00:00", "", "Add", "19743422 [REDACTED]6"
"Mark M [REDACTED].5", "Incoming - Missed Call, unopened", "[REDACTED]", "017 [REDACTED]", "2009/08/
14: [REDACTED]:01", "2009/08/06 16:38:09", "00:00:00", "", "Add", "197434224 [REDACTED]9"

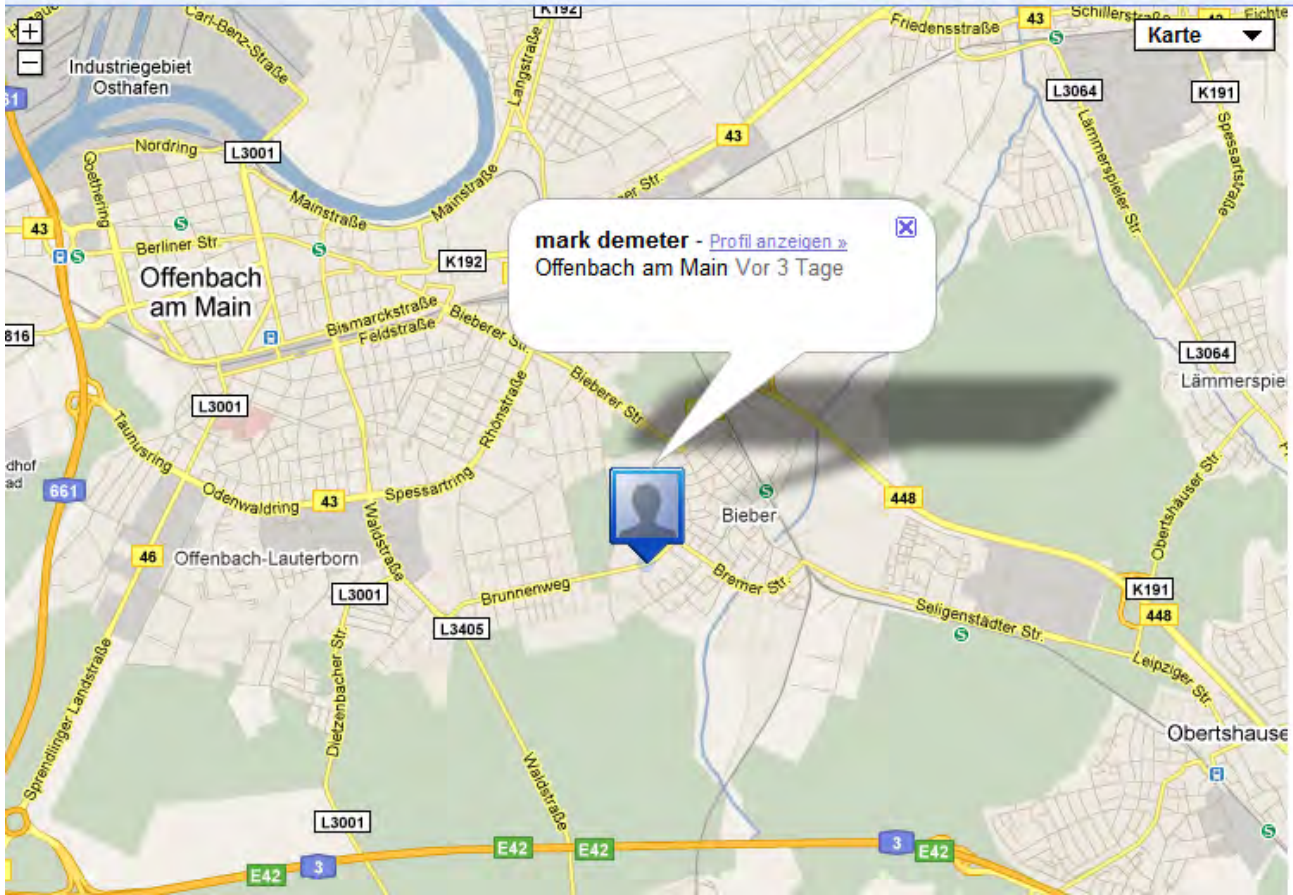
```



BB-Nutzer Richtung Dauer Name Rufnummer Zeitpunkt

- GPS - das „Global Positioning System“ für die Navigation
- ist heute in immer mehr Geräten eingebaut
- Es gibt kaum noch ein Handys ohne GPS
- Über einen Rückkanal (SMS, E-Mail, Handy-Datenverbindung) lassen sich diese GPS-Daten aus der Ferne auslesen - auch heimlich
- Damit kann für jeden Mitarbeiter ein lückenloses Bewegungsprofil erstellt werden
- Wird bei Logistik-Unternehmen oft standardmäßig für das Flottenmanagement eingesetzt, aber auch bei Taxen, Außendienstmitarbeitern etc.

Überwachung von Bewegung: Latitude - Demo



28.04.2011

Standortsuche für Radarfallen

TomTom entschuldigt



Navigationsgerät: TomTom setzt künftige

Die Kunden sind wütend: In den Niederlanden hat der Hersteller TomTom erfasste Geschwindigkeitsdaten an die Polizei verkauft. Die will überall Radarfallen installieren. Informationen statistisch viel genauer

SPIEGEL ONLINE

06. Mai 2011, 14:22 Uhr

Standortsuche für Radarfallen

TomTom verärgert australische Autofahrer

Die Navi-Nutzer in den Niederlanden haben sich vor wenigen Tagen noch darüber beklagt, dass TomTom ihre GPS-Daten an die Polizei verkauft hatte. Das Unternehmen entschuldigte sich dafür - und verhandelt nun mit Behörden in Australien.

TomTom bringt erneut Navi-Nutzer gegen sich auf: [Gegenüber der Nachrichtenseite "The Australian Financial Review"](#) hat das Unternehmen zugegeben, GPS-Aufzeichnungen von Geräten australischer Kunden an den Meistbietenden verkaufen zu wollen. TomTom schließt dabei nicht aus, die Informationen auch den australischen Behörden anzubieten. Der Marketing-Vizechef des Unternehmens, Chris Kearney, sagt: "Wir haben mit einigen Forschungseinrichtungen in Australien gesprochen, die eng mit der Regierung zusammenarbeiten."

Alle TomTom-Geräte, die in den letzten drei Jahren in Australien verkauft wurden seien so konstruiert, dass sie Aufzeichnungen über gefahrene Routen, Fahrzeiten und Geschwindigkeiten an den Hersteller übermitteln. Ursprünglich hatte das Unternehmen dieses Datenabgleich damit begründet, dass die Aufzeichnungen genutzt werden sollen, um die Streckenführung der Geräte zu optimieren. TomTom vermarktet eine entsprechende Funktion seiner Navigationsgeräte unter dem Namen IQ Routes.

In den Niederlanden hatte TomTom mit ähnlichen Geschäften bereits **in der vergangenen Woche seine Kunden verärgert**. Das Unternehmen hatte der dortigen Polizei ebenfalls GPS-Aufzeichnungen seiner Kunden verkauft. Anhand der gespeicherten Geschwindigkeiten und der zugehörigen Ortsangaben plant die Polizei dort nun, geeignete Stellen für Radarfallen zu ermitteln. Denn aus den Informationen lässt sich herauslesen, auf welchen Strecken die Autofahrer am häufigsten rasen.

Für diese Aktion hat sich Unternehmenschef Harold Goddijn bereits öffentlich entschuldigt. Man sei davon ausgegangen, dass die Daten benutzt werden, um den Verkehr auf den Straßen sicherer zu machen, sagte Goddijn. Auch versicherte das Unternehmen, dass die Daten der Nutzer anonym ausgelesen werden. Einem Sprecher des Unternehmens zufolge können Raser anhand der ausgelesenen Daten nicht im Nachhinein identifiziert werden. Auch sei es nicht möglich, die gefahrenen Strecken einem bestimmten Navi-Nutzer zuzuordnen.

jbr

Überwachung von Bewegung: Beispiele aus Social Networks

The image shows a screenshot of the Gowalla website. The search bar contains 'frankfurt'. Below the search bar, there are statistics for 'Frankfurt Airport': 2,087 People, 4,468 Check-ins, 116 Photos, and 6 Highlights. A list of spots is shown, including 'FRA Frankfurt International', 'Hauptbahnhof Frankfurt am M', and 'Fernbahnhof Frankfurt am Ma'. A red arrow points from the 'FRA Frankfurt International' spot to a detailed view of a flight check-in. The detailed view shows a user profile, a photo of the airport terminal, a distance of 4,293 km, and a post by 'Wael Hazzazi' who flew out of 'RUH King Khalid International' and arrived at 'FRA Frankfurt International' 12 minutes ago. Another post by 'Lamees Al Kindi' is also visible.

Spot	People	Check-ins
FRA Frankfurt International	2087	4468
Hauptbahnhof Frankfurt am M	884	3822
Fernbahnhof Frankfurt am Ma	359	730
FRA Terminal 2	312	582

Category	Count
People	2,087
Check-ins	4,468
Photos	116
Highlights	6

Quelle: www.gowalla.com

Internet-Telefonie (Voice over IP - VoIP)

- Statt der klassischen Punk-zu-Punkt Telefonleitung eine virtuelle VoIP-Verbindung
- Die Datenübertragung erfolgt über das Internet (ähnlich E-Mail und WWW)
- Bei Privatpersonen und Unternehmen inzwischen sehr weit verbreitet
- Standardisiert: SIP
- Keine Verschlüsselung im Standard vorgesehen!

Mitschnitt von Daten

- Der gesamte Datenverkehr kann mitgeschnitten werden

The screenshot shows a Mozilla Firefox browser window titled "FRITZ!Box Paketmitschnitt". The address bar shows the URL "http://fritz.box/cgi-bin/webcm?getPage=../html". The page content includes instructions for starting a packet capture. A red circle highlights the "Start" and "Stop" buttons under the heading "Paketmitschnitt auf DSL-Ebene (Standard):". A red arrow points from the "Start" button to a "Speichern unter" (Save As) dialog box. The dialog box shows the file name "fritzbox-vc0.eth" and the file type "Alle Dateien".

FRITZ!Box Paketmitschnitt

FRITZ!Box kann zur Diagnose alle Pakete, die über DSL oder im Modus "Internetzugang über DSL" verschickt werden, im Wireshark-Format mitschneiden. Starten Sie den Mitschnitt über die Start-Schaltfläche und speichern Sie die Datei auf der Festplatte. Zum Beenden des Mitschnitts drücken Sie die Stop-Schaltfläche.

Wichtig: Brechen Sie nicht den Download im Browser ab, wenn Sie den Mitschnitt beenden möchten. Drücken Sie die entsprechende Stop-Schaltfläche.

FRITZ!Box Packet Trace FRITZ!Box can trace all packets sent via DSL or in "Internet access over DSL" mode in Wireshark format. Start the packet trace by clicking the corresponding Start button and save the file to the hard disk. Click the "Stop" button to end the trace.

Important: Do not interrupt the download in the browser to end the trace! Click the corresponding Stop button instead.

Paketmitschnitt auf DSL-Ebene (Standard):
Packet trace on the DSL level (default):

Start Stop

Angehalten

Speichern unter

Speichern in: fritz

Eigene Dateien
Arbeitsplatz
Desktop
(N:) Daten auf "mamis-server"
Netzwerkumgebung

Dateiname: fritzbox-vc0.eth
Dateityp: Alle Dateien

Speichern
Abbrechen

- Im Datenmitschnitt können die VoIP-Telefonate herausgesucht und als Audio-Datei abgespielt werden

The screenshot displays the Wireshark interface with a packet capture from 'fritzbox-vcc0.eth'. The left pane shows a list of packets, with packet 17 (SIP) circled in red. The middle pane shows the protocol hierarchy for the selected packet, highlighting 'SIP' and 'VoIP Calls'. The right pane shows the 'VoIP - RTP Player' window, which displays two audio waveforms. The top waveform is labeled 'From 62.53.226.81:16808 to 89.14.162.13:7078 Duration:47,36 Drop by Jitter Buff:0(0,0%) Out of Seq: 1(0,0%)'. The bottom waveform is labeled 'From 89.14.162.13:7078 to 62.53.226.81:16808 Duration:44,22 Drop by Jitter Buff:0(0,0%) Out of Seq: 0(0,0%)'. The RTP Player window includes a 'Jitter buffer [ms]' set to 50 and buttons for 'Decode', 'Play', 'Pause', 'Stop', and 'Close'.

Foto: Screenshot „Wireshark“ (www.wireshark.org)

SPIEGEL ONLINE

15. September 2010, 11:33 Uhr

Verletzter Datenschutz

Google-Mitarbeiter spionierte Teenager aus

Google hat einen Mitarbeiter entlassen, der unbefugt persönliche Nutzerdaten abgerufen haben soll. Einem Medienbericht zufolge hat der Mann Chat-Protokolle eingesehen und Gespräche belauscht. Der Vorfall zeigt, wie leicht Mitarbeiter des Konzerns an persönliche Daten kommen können.

Der Suchmaschinenkonzern [Google](#) hat bestätigt, dass der Konzern einen 27-jährigen Software-Entwickler entlassen hat. Einem Bericht des [Medienblogs Gawker.com](#) zufolge soll der Gefeuerte mehrfach persönliche Google-Konten ohne Zustimmung der Nutzer eingesehen haben. In mindestens vier Fällen habe es sich dabei um die Konten Minderjähriger gehandelt.

Gawker.com zitiert eine nicht näher genannte Quelle innerhalb des Unternehmens. Demnach hat der 27-Jährige private Chatverläufe gelesen und Gespräche über den Internet-Telefonie-Dienst Google Voice mitgehört. Im Anschluss habe er seine Opfer darauf hingewiesen, dass er sie ausspionierte hatte. In einem Fall habe er einen 15-Jährigen damit verhöhnt, den Namen und die Telefonnummer von dessen neuer Freundin zu kennen. In einem anderen Fall habe der

- Spionage-Software basiert auf dem Prinzip der Key-Logger, sie protokolliert jeden Tastendruck eines PCs und mehr:
 - Regelmäßige Screenshots des Desktop, die später wie ein Videofilm abgespielt werden können. Manchmal auch zusätzliches Bild des Benutzers per WebCam
 - Assoziation der Tasteneingaben mit Anwendungen
 - Alarm-Funktionen bei „bösen Wörtern“ oder Anwendungen
 - Restriktionsmöglichkeiten (bspw. kann das Öffnen von bestimmten Programmen unterbunden werden)
 - Versand der Protokolle und/oder Warnungen per Mail
 - Spionage-Software arbeitet oftmals in einem „Silent-Mode“ und ist durch den Benutzer nicht zu finden

Überwachung des Desktop: Spionage-Software - Beispiel

Aufzeichnungsmenü (noch 6 Tage bis Ablauf der Lizenz) [BENDERIX]

Oktober 2008

Mo	Di	Mi	Do	Fr	Sa	So
29	30	1	2	3	4	5
6	7	8	9	10	11	12
13	14	15	16	17	18	19
20	21	22	23	24	25	26
27	28	29	30	31	1	2
3	4	5	6	7	8	9

Today: 31.10.2008

All In One Keylogger Log Viewer

Benut...	Zeitfenster	aktives Fenster
jensm	10/30/2008 19:56:36	about:Tabs - Windows Internet Explorer
jensm	10/30/2008 19:56:36	Registerbrowsen - Windows Internet Explorer
jensm	10/30/2008 19:56:47	1&1 Webmailer - Windows Internet Explorer
jensm	10/30/2008 19:57:23	Keylogger Dialog
jensm	10/30/2008 19:57:23	1&1 Webmailer - Windows Internet Explorer
jensm	10/30/2008 19:57:36	All In One Keylogger™ V 3.1 (noch 7 Tage bis Ablauf der Lizenz)
jensm	10/30/2008 19:57:41	Keylogger Dialog
jensm	10/30/2008 19:57:44	Aufzeichnungsmenü (noch 7 Tage bis Ablauf der Lizenz) [BENDERIX]
jensm	10/30/2008 20:00:29	Download Keylogger & Spy Software, Download All In One Keylogger fr...
jensm	10/30/2008 20:00:33	Google Chrome
jensm	10/30/2008 20:00:34	Keylogger Download Keylogger, Download freie Testversion, Kostenlose...
jensm	10/30/2008 20:01:07	Microsoft PowerPoint - [2008-11-04_BigBrother Hamburg.ppt [Kompatibilit...
jensm	10/30/2008 20:01:36	Microsoft PowerPoint
jensm	10/30/2008 20:01:36	Keylogger Download Keylogger, Download freie Testversion, Kostenlose...
jensm	10/30/2008 20:01:39	Monitoring, Virenschutz und Zugriffskontrolle für Microsoft ISA Server - ...

1&1 Webmailer - Windows Internet Explorer

test@mainis.de test

geheim

Kennwort-Mitschnitt

Tastatur-Mitschnitt

Zeitpunkt

Aufgerufenes Programm

Überwachung des Desktop: Spionage-Software - Demo

RelyTec English | F

All In One Keylogger™

All In One Keylogger Special Features

- Captures all keystrokes (Keystrokes Recorder),
- Records instant messengers,
- Monitors application usage,
- Captures desktop activity,
- Captures screenshots,
- Quick search over the log,
- Sends reports via e-Mail, FTP, Network, Rec
- microphone sounds,
- Generate HTML reports,
- Disable Anti Keyloggers,
- Disable unwanted softwares,
- Filter monitored user accounts,
- Captured screenshots "Slide Show",
- Sends reports by FTP,
- Sends reports in HTML format,
- Blocks unwanted URLs,
- Stops logging when computer is Idle.

New - Invisible in Task Manager (All Windows Versions),

New - Captures mouse Cursor,

New - Support for Dual Monitor,

New - Sends Logs Via Network,

New - Advanced Search for Log Viewer,

New v2.8 Full support for Windows Vista,

New v2.8 Captures snapshots of semi transparent windows,

New v2.9 Visual Surveillance filtering,

New v2.9 Support for Firefox web monitoring In addition to Internet Explorer,

New v2.9 Takes screenshot when one of predefined keywords is typed,

New v3 Auto Uninstall at a specific date,

New v3 Automatically flushes logs to a USB stick,

New v3 Textual Surveillance filtering,

New v3 Keylogger was translated to Czech (Cestina),

New v3.1 2-Sides IM Logging,

New v3.1 Option to set Keylogger to capture only the

All In One Keylogger offers you advanced features at affordable

Features :

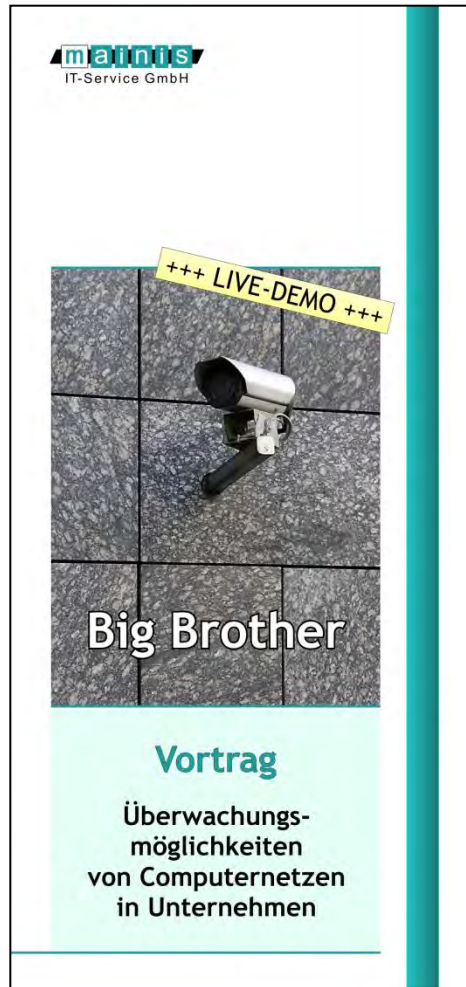
- Applications and keystro**
Do they write letters in W
That makes absolutely no
Our Keylogger can record
This, combined with the vi
Our Keylogger even enable
- Web Logging**
Do your children spend a lo
Do you ever wonder what
Do you want to know if yo
- Chat Logging**
Do your children spend a lo
Do you ever wonder with v
Do they take secret chat

Disable Anti Keyloggers.

New - Invisible in Task Manager (All Windows Versions).

New v2.9 Takes screenshot when one of predefined keywords is typed.

Weitere Informationen und Kontakt



The poster features the 'mainis IT-Service GmbH' logo at the top left. Below it is a photograph of a silver and black security camera mounted on a wall. A yellow banner with the text '+++ LIVE-DEMO +++' is placed over the top of the camera. The words 'Big Brother' are written in a large, white, sans-serif font across the bottom of the camera image. At the bottom of the poster, the word 'Vortrag' is written in a teal font, followed by the text 'Überwachungsmöglichkeiten von Computernetzen in Unternehmen' in a smaller black font.



mainis IT-Service GmbH
Erich-Ollenhauer-Str. 24
63073 Offenbach am Main
Tel. 069/86007057
info@mainis.de
www.mainis.de

Alle im Vortrag verwendeten Produkt- und Firmennamen sind eingetragene Warenzeichen der jeweiligen Inhaber