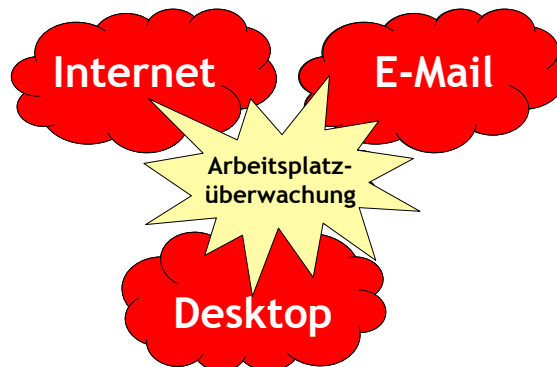


*Machen Sie doch, was Sie wollen...
Wir helfen Ihnen dabei.*

Gerrit Wiegand, Jens Möisinger

**Gefährdungspotenziale
elektronischer Kommunikation**
- eine Demonstration
der Möglichkeiten in der Praxis

im Rahmen der ver.di-Betriebsrätemesse
am 27. und 28. September 2004 in Berlin

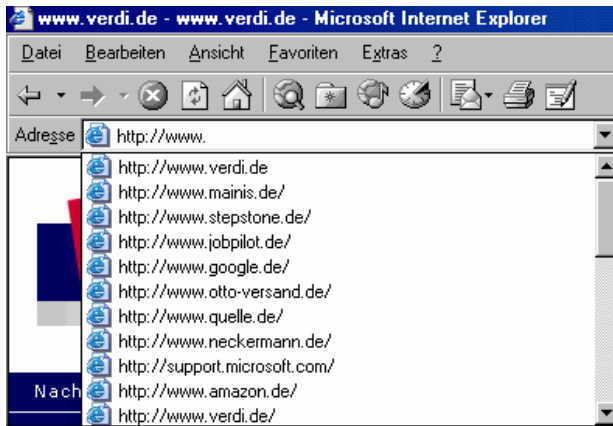


Lokale Überwachung von Internet-Aktivitäten

- Lokale Überwachung bedeutet:
 - Auswertung der auf einem bestimmten PC entstehenden Datenspuren
 - I.d.R. nur am Gerät selbst oder per Laufwerkszugriffe möglich und damit aufwändig
 - Für unternehmensweite oder präventive Überwachung nur bedingt geeignet, eher für Einzelfall-Kontrollen oder „neugierige Kollegen“
- Viele Internet-Anwendungen hinterlassen „standardmäßig“ Datenspuren, z.B.
 - Cookies
 - Browser-Cache
 - History-List



Lokale Überwachung von Internet-Aktivitäten: History-List - Demo



- Abhilfe: Die Liste kann in den meisten Browsern in den Einstellungen gelöscht werden („Verlauf“ oder „Historie“)



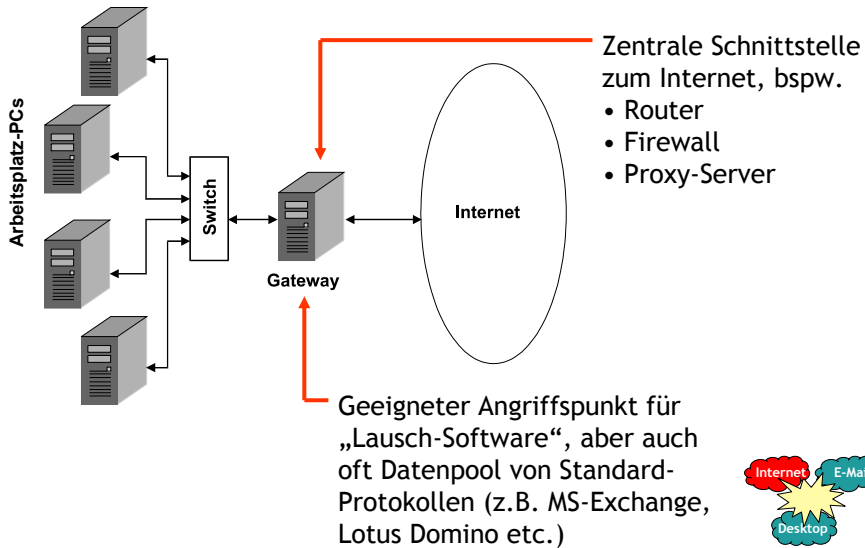
Fotos: Screenshot Microsoft Internet-Explorer

Zentrale Überwachung von Internet-Aktivitäten

- Zentrale Überwachung bedeutet:
 - Die Daten werden an einem zentralen Punkt gesammelt (dem „Internet-Gateway“)
 - Sie sind unabhängig vom einzelnen Arbeitsplatzrechner auswertbar
 - Sie können für zentrale Auswertungen und auch für präventive Überwachungen komfortabel eingesetzt werden
- Oft sind solche Protokolle für einen reibungslosen Betriebsablauf notwendig, meistens werden sie aber auch nur gedankenlos mitgeschrieben
- Es gibt aber auch Spezial-Software, die nur für diesen Zweck entwickelt wurde und entsprechend leistungsfähig ist



Zentrale Überwachung von Internet-Aktivitäten (II)



Zentrale Überwachung von Internet-Aktivitäten: 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



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\qerrit(89)
www.msn.de	57	html:4 jpg:15 gif:35	1	frater-magnus\qerrit(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\{S} 127.0.0.1(S)
www.verdi-bildungsportal.de	2		1	frater-magnus\qerrit(2)
www.macromedia.com	2		1	frater-magnus\qerrit(2)
www.adobe.de	2		1	frater-magnus\qerrit(2)
magnus.frater-magnus.local	1	html:1	1	frater-magnus\administrator(1)
www.google.de	2	html:1 gif:1	1	frater-magnus\qerrit(2)
www.microsoft.com	1	html:1	1	frater-magnus\qerrit(1)
emealoin.msn.com	1	html:1	1	frater-magnus\qerrit(1)
msid.eu.msn.com	1	html:1	1	frater-magnus\qerrit(1)
a.faa.de	4	html:1 gif:1	1	frater-magnus\qerrit(4)
msn.ivwbox.de	2	gif:1	1	frater-magnus\qerrit(2)
c.msn.de	1	gif:1	1	frater-magnus\qerrit(1)
ad.de.doubleclick.net	3	html:1 flash:1	1	frater-magnus\qerrit(3)
www.passportimages.com	1	gif:1	1	frater-magnus\qerrit(1)
global.msads.net	1	gif:1	1	frater-magnus\qerrit(1)

Aufgerufene
Seiten,
hier:

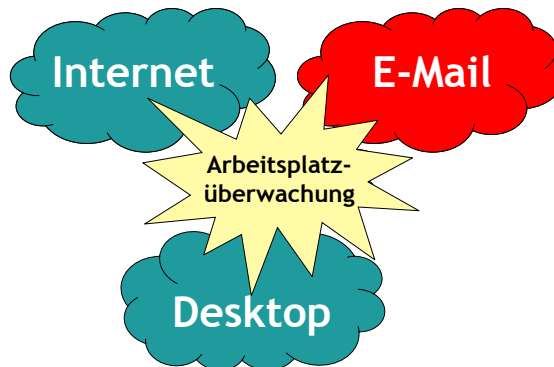
- ver.di
- Adobe
- Google

Anzahl Aufrufe
pro Benutzer

Benutzername



Fotos: Screenshot GFIWebMonitor (www.gfi.com)

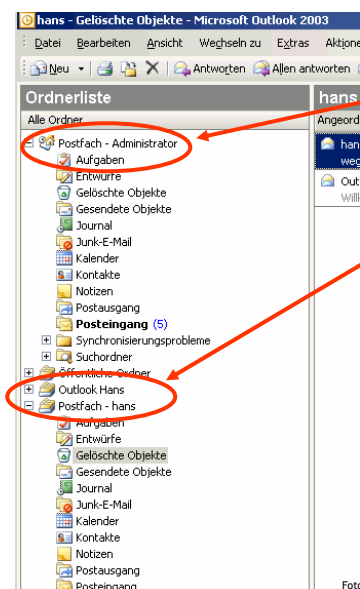


Lokale Überwachung von E-Mail-Aktivitäten

- 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



Zentrale Überwachung von E-Mail-Aktivitäten (II)

- „Unbewusste“ Überwachung des E-Mail-Verkehrs
- „Indirekte“ Überwachung durch Spam-Filter
 - Spam-Filter „lesen“ jede E-Mail, um unerwünschte Werbe-E-Mails herausfiltern zu können
 - Dazu ist die Analyse des Inhalts (Worte, Zeichen, Bilder etc.) notwendig
 - Die meisten Spam-Filter protokollieren ihr Vorgehen
 - Spam-Filter gewinnen eine immer größere Bedeutung in Unternehmen
- „Gezielte“ Überwachung durch E-Mail-Filter



Zentrale Überwachung von E-Mail-Aktivitäten: „Indirekt“: Demo GFI-MailMonitor

A screenshot of the GFI MailEssentials Monitor software interface. The window title is 'GFI MailEssentials Monitor'. It shows a list of processed emails with columns for date, time, subject, sender, and recipient. Red arrows point to specific fields in the log, labeled with German terms: 'Betreff' (Subject), 'Absender' (Sender), and 'Empfänger' (Recipient). The log entries include details such as 'Subject: AW: Bittere Wahrheit?!', 'Sender: [redacted]@aventis.com', and 'Recipient: mark@mainis.local'. The interface also shows a menu bar with 'File' and 'Help', and a status bar at the bottom with the text 'Fotos: Screenshot GFI MailEssentials Monitor (www.gfisoftware.de)'.

Number of emails processed: 585

GFI MailEssentials | POP2Exchange

Betreff

Absender

Empfänger

Betreff

Absender

Empfänger



Zentrale Überwachung von E-Mail-Aktivitäten (III)

- „Unbewusste“ Überwachung des E-Mail-Verkehrs
- „Indirekte“ Überwachung durch Spam-Filter
- „Gezielte“ Überwachung durch E-Mail-Filter
 - Auswertung des unternehmensweiten E-Mail-Verkehrs
 - Umfangreiche Protokoll- und Alarm-Funktionen
 - Restriktionsmöglichkeiten:
 - Beschränkungen auf bestimmte Mail-Empfänger
 - Beschränkungen auf bestimmte Arten von Anhängen
 - Beschränkungen bei der Größe der Mails etc.

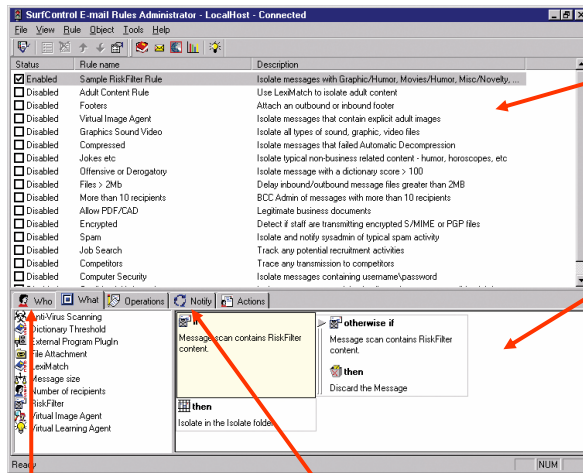


Zentrale Überwachung von E-Mail-Aktivitäten: E-Mail-Filter-Software

- E-Mail-Filter-Software ermöglicht
 - Das Beschränken des E-Mail-Verkehrs
 - Suche nach „bösen Wörtern“
 - Teilweise werden auch Anhänge untersucht, teilweise sogar Bilder interpretiert
 - Sperrung von verdächtigen Mails möglich
 - Automatische Benachrichtigung von Administratoren bei verdächtigen Mails möglich
- Weit verbreitete Anwendungen:
 - SuperScout E-Mail-Filter (SurfControl GmbH)
 - Orangebox Mail (Cobion AG)
 - Mail-Gear (Symantec)



Zentrale Überwachung von E-Mail-Aktivitäten: E-Mail-Filter-Software - Demo



Liste der Ereignisse, z.B.

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

Verfahrensanweisungen
beim Zutreffen einer
Regel, z.B.

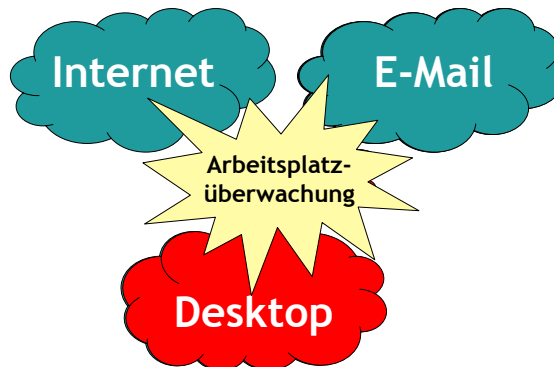
- „Löschen“
- „Zurückschicken“
- „Zwischenspeichern“

Benutzerabhängige
Regeln

Automatische
Benachrichtigungen



Foto: Homepage der Firma „SurfControl“ (www.surfcontrol.com)

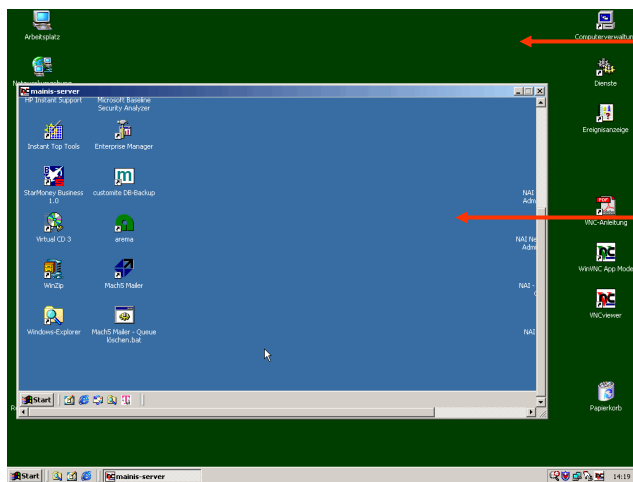


Überwachung des Desktop: Fernwartungs-Zugriffe

- 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 vor der Verbindung gefragt, ob er ihr 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



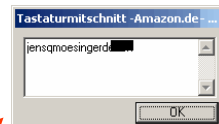
Überwachung des Desktop: Spionage-Software

- Spionage-Software basiert auf dem Prinzip der Key-Logger, sie protokolliert jeden einzelnen 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 somit durch den Benutzer nicht zu identifizieren



Überwachung des Desktop: Spionage-Software - Demo

Fenstertitel	Startzeit	Ungefähre Zeit	LK
Tastaturmitschnitt - Kontoführung im Internet - Login 50650023 - Microsoft Inte	04.09.2002 14:47:31	(00:00:04)	
Tastaturmitschnitt - Finanzportal-Main-Kinzig.de :: Sparkasse Hanau - Micro	04.09.2002 14:47:35	(00:00:05)	
Kontoführung im Internet - Abmeldung 50650023 - Microsoft Internet Explorer	04.09.2002 14:48:24	(00:00:12)	Txt
Amazon.de: Willkommen - Microsoft Internet Explorer	04.09.2002 14:48:35	(00:00:04)	
Amazon.de: - Microsoft Internet Explorer	04.09.2002 14:48:38	(00:00:24)	
Amazon.de Einkaufswagen - Microsoft Internet Explorer	04.09.2002 14:49:01	(00:00:06)	
Amazon.de Anmeldung - Microsoft Internet Explorer	04.09.2002 14:49:06	(00:00:20)	Txt
Amazon.de Einkaufswagen - Microsoft Internet Explorer	04.09.2002 14:49:25	(00:00:06)	Txt
Dokument1 - Microsoft Word	04.09.2002 14:51:02	(00:00:01)	
...Dokument1	04.09.2002 14:51:02	(00:00:02)	
...MsoDockTop	04.09.2002 14:51:03	(00:00:18)	Txt



Kennwort-Mitschnitt



Word-Mitschnitt

Aufgerufenes Programm

Zeitpunkt

Verweildauer



Weitere Informationen und Kontakt



- **Ratgeber „Der Chef surft mit“**
www.onlinerechte-fuer-beschaefigte.de



- **Im Netz@work**
Michael Sommer / Cornelia Brandt / Lothar Schröder
VSA-Verlag, ISBN 3-87975-880-8, EUR 12,80



- **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