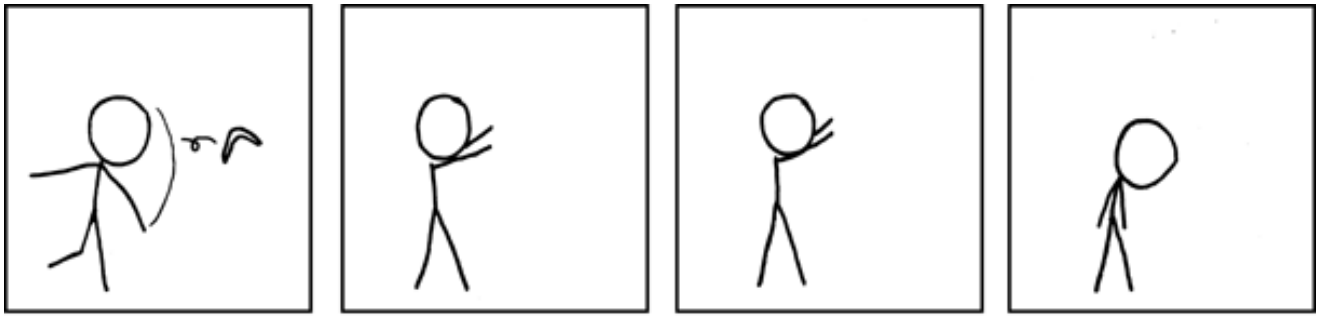
Can Data Leakage Prevention Prevent Data Leakage?



Matthias Luft

mluft@informatik.uni-mannheim.de

University of Mannheim, Germany
Laboratory for Dependable Distributed Systems

Agenda

- Motivation
- Definitionen
- Ziele
- Testreihe
- Ergebnisse
- Zusammenfassung

Motivation

04.10.2008 Drucken | Senden | Bookmark | Feedback | Merken

TELEKOM-SKANDAL Schrift: +

Diebe klauten 17 Millionen T-Mobile-Kundendatensätze

News › Politics › Terrorism policy

Ebay camera contains 'secret' MI6 terrorist images

New owner finds photos of images of launchers, missiles, terror suspects and their details on camera

E-mail this to a friend Printable version

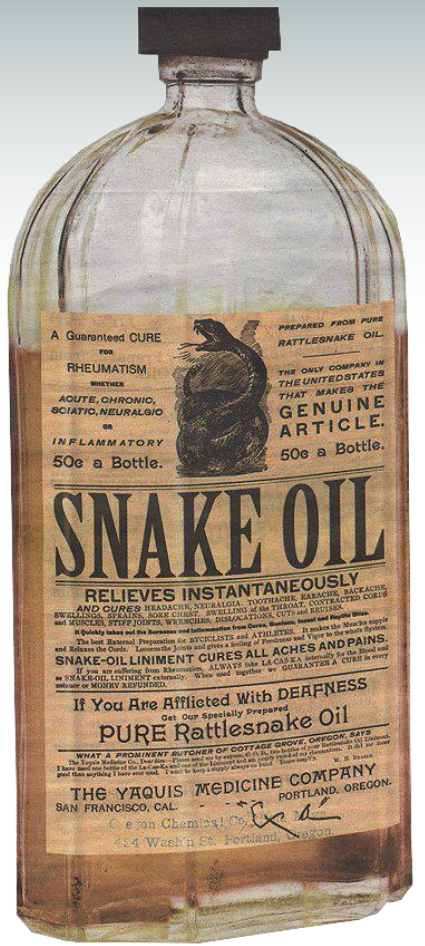
Teachers' details on missing disk

A computer disk containing the names and addresses of more than 11,000 teachers has gone missing in the post.

University of Mannheim, Germany
Laboratory for Dependable Distributed Systems

Meine Motivation

- Potenzielles *Snakeoil*
- Extrem hohe Komplexität
- Vielschichtige Lösung
  - Endgeräte
  - Netzwerkkomponenten
  - *Application Gateways* (Email, Web)



Definition

Data Leakage Prevention ist

Auf zentralen Richtlinien basierende

Überwachung

und Identifikation

von Daten in

Bewegung

Ruhe

Benutzung

Definition *Leakage*

Data Leakage is – from the owner's point of view – unintentional loss of confidentiality for any kind of data

Ziele

- Schwachstellen in DLP Lösungen finden
- Aber: Was sind Schwachstellen im Bezug auf DLP?

➢ Folgende Fragestellungen:
  - ➢ Ist zufällige Leakage möglich?
  - ➢ Ist es möglich die Sicherheitsmechanismen zu umgehen?
  - ➢ Enthält das Design der Lösungen Fehler?

Exemplarische Testfälle

- Werden sensible Daten zuverlässig erkannt?
- Werden unbekannte Datenstrukturen untersucht?
- Werden alle externen Geräte überwacht?
- Wie wird auf erkannte Policy-Verstöße reagiert?
- Werden verschlüsselte Kanäle zur Kommunikation genutzt?

Untersuchte Lösungen

- Fokus auf Untersuchung der Überwachung von Wechselmedien

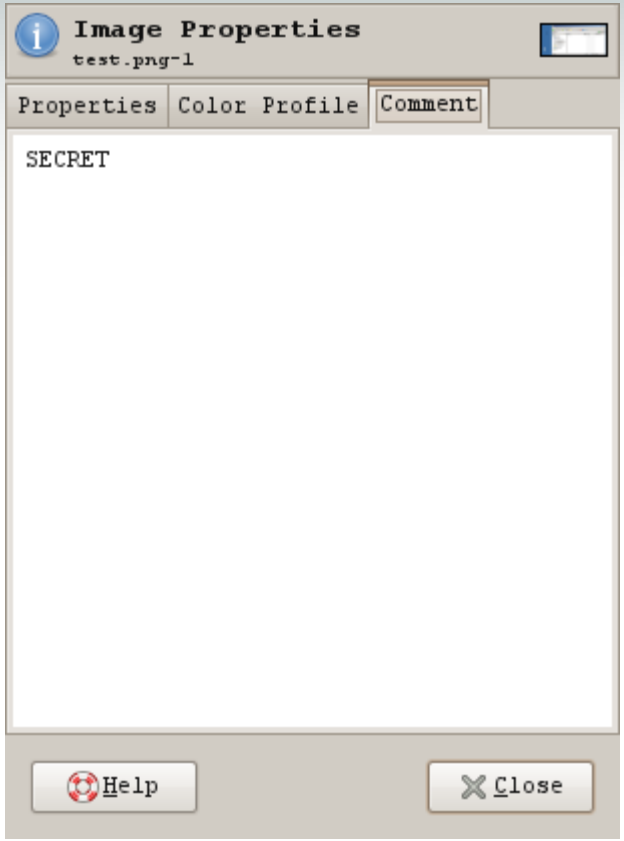
- McAfee Host Data Leakage Prevention
  - Sehr neues Produkt

- Websense Data Security Suite
  - Eines der ältesten Produkte

Test- und Ergebnisüberblick

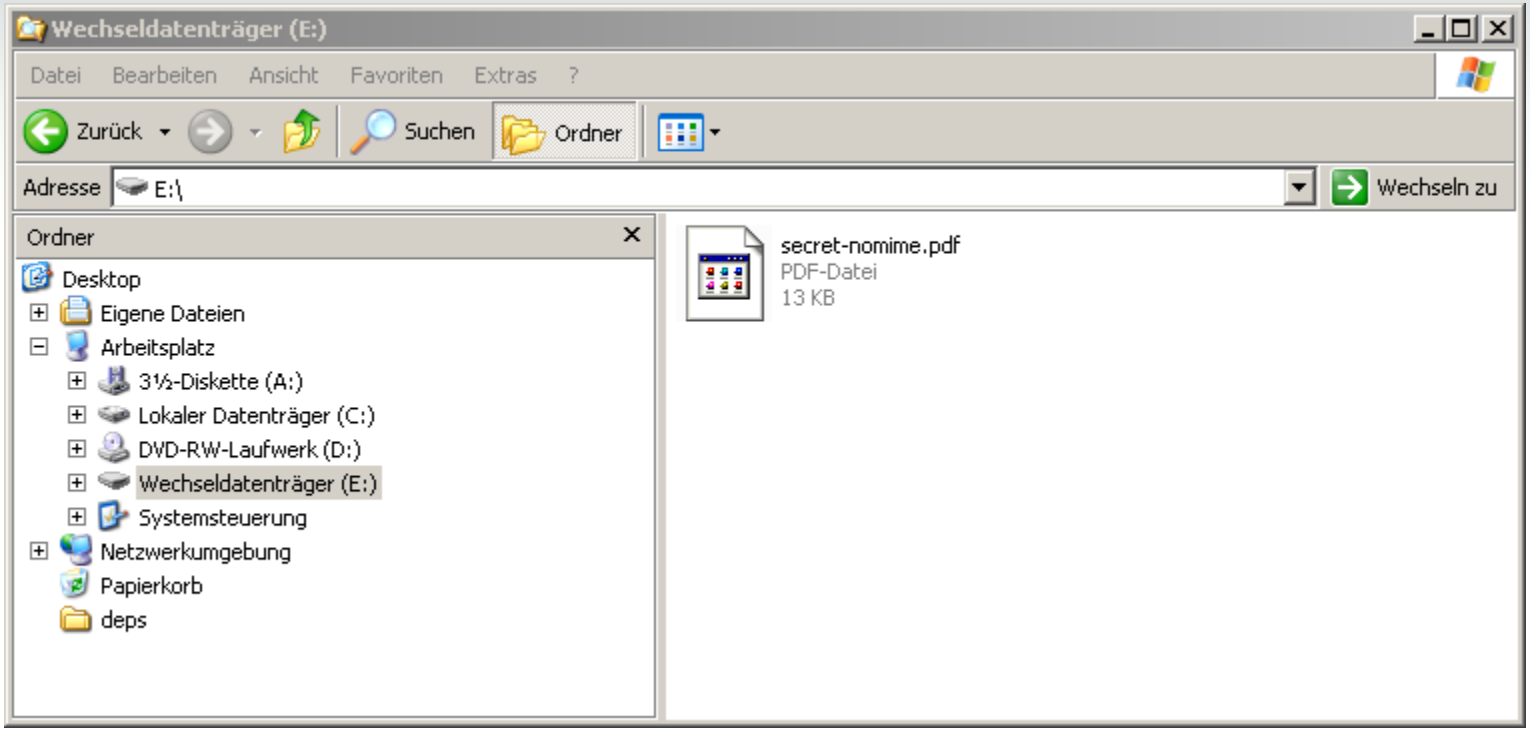
Test	McAfee	Websense
Textdatei		
Dateiname		
PDF		
Word/Excel Einbettungen		
Komprimierung		
Unbekannter MIME Type		
Metadaten		
NTFS Alternate Data Stream		
Third Party Filesystems		
Mehrere Partitionen		
Sichere Reaktion		
Verschlüsselung		
Fuzzing		
Große Dateien		

Exemplarische Ergebisse



University of Mannheim, Germany
Laboratory for Dependable Distributed Systems

Exemplarische Ergebnisse

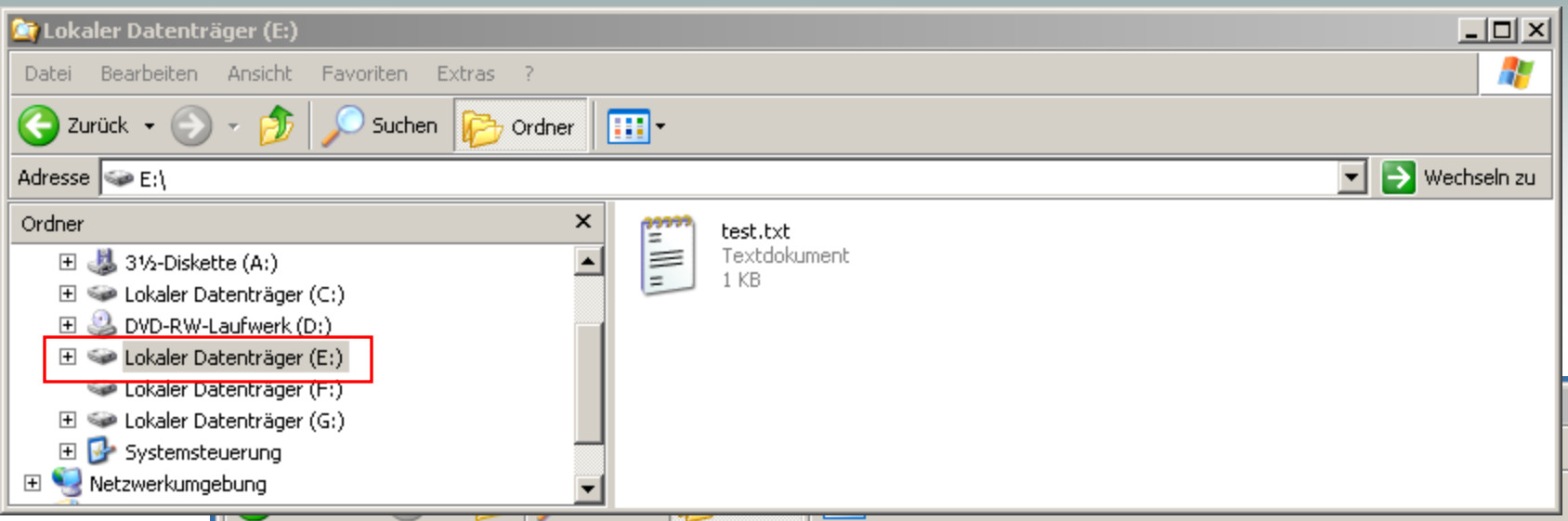


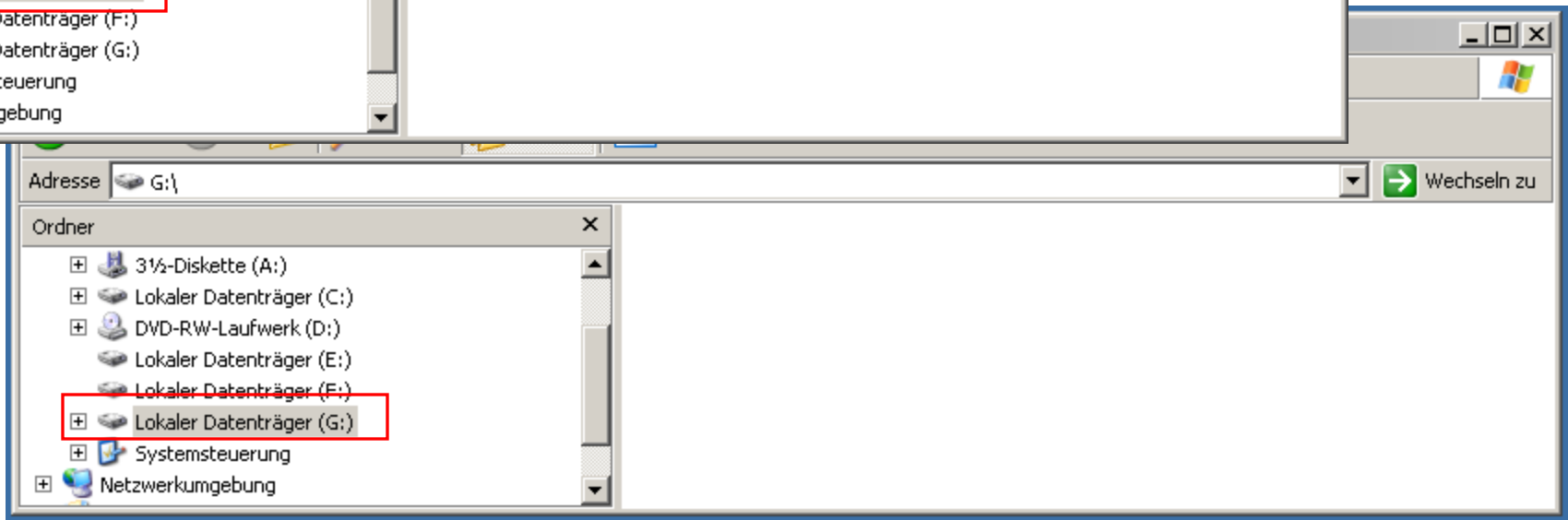
McAfee

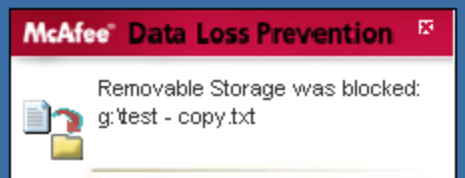
File Edit View Terminal Go Help

```
bender ~ # xxd /dev/fd0 | grep -i secret
0004200: 5345 4352 4554 5345 4352 4554 5345 4352  SECRETSECRETSECR
```

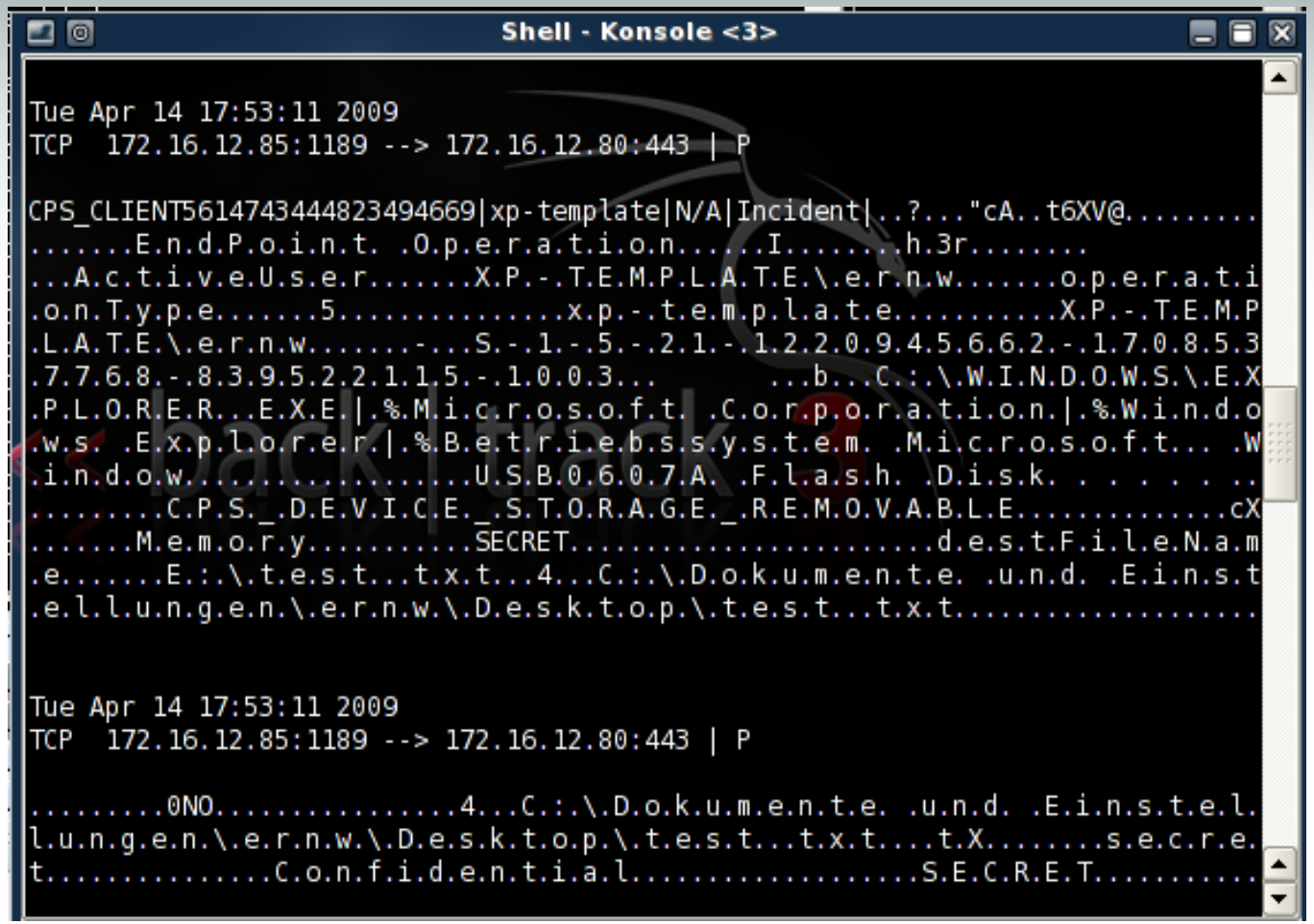
McAfee


Lokaler Datenträger (E:)
Datei Bearbeiten Ansicht Favoriten Extras ?
Zurück Suchen Ordner
Adresse E:\
Wechseln zu
Ordner
3½-Diskette (A:)
Lokaler Datenträger (C:)
DVD-RW-Laufwerk (D:)
Lokaler Datenträger (E:)
Lokaler Datenträger (F:)
Lokaler Datenträger (G:)
Systemsteuerung
Netzwerkumgebung
test.txt
Textdokument
1 KB


Adresse G:\
Wechseln zu
Ordner
3½-Diskette (A:)
Lokaler Datenträger (C:)
DVD-RW-Laufwerk (D:)
Lokaler Datenträger (E:)
Lokaler Datenträger (F:)
Lokaler Datenträger (G:)
Systemsteuerung
Netzwerkumgebung


McAfee Data Loss Prevention
Removable Storage was blocked:
g:\test - copy.txt

Websense



University of Mannheim, Germany
Laboratory for Dependable Distributed Systems

Websense

- Kompletter System Freeze bei Kopieren einer 5GB Datei
  - reproduzierbar

Zusammenfassung

- Beide Lösungen enthalten gravierende Schwachstellen
  - Abwägung Nutzen/Risiko?
  - Beide Hersteller haben bis heute noch nicht reagiert
- Further work
  - Untersuchung weiterer Lösungen
  - Tiefergehende Untersuchungen
  - Ausarbeitung einer DLP Testmethodik/-liste

Danke für die Aufmerksamkeit!

University of Mannheim, Germany
Laboratory for Dependable Distributed Systems

Fragen?

University of Mannheim, Germany
Laboratory for Dependable Distributed Systems