

A small leak will sink a great ship: An Empirical Study of DLP solutions

Matthias Luft, Thorsten Holz

{mluft|thorsten.holz}@informatik.uni-mannheim.de

Agenda

Problem Statement

Motivation

Key Concepts

Evaluation Criteria & Test Cases

Evaluation Results

Problem Statement

To lose controls over one's own data is the primal fear of the digital age.

Organizations and individuals want to prevent leakage of

- Trade secrets (“the Coca Cola formula”)
- Marketing plans / financial data
- Data that is regulated by laws (e.g. HR data)
- Data to be protected for some flavor of “compliance” (credit card nos.)
- Embarrassing stuff (your private poems from adolescence ;-)

Case Studies

Eli Lilly E-Mail to New York Times - Portfolio.com - Windows Internet Explorer

http://www.portfolio.com/news-markets/top-5/2008/02/05/Eli-Lilly-E-Mail-to-New-York-Times


Datei Bearbeiten Ansicht Favoriten Extras ?

Eli Lilly E-Mail to New York Times - Portfolio.com

Lilly's \$1 Billion E-Mailstrom

by Katherine Eban | Feb 5 2008

A secret memo meant for a colleague lands in a *Times* reporter's in-box.



When the *New York Times* broke the story last week that [Eli Lilly & Co.](#) was in confidential settlement talks with the government, angry calls flew behind the scenes as the drug giant's executives accused federal officials of leaking the information.

As the company's lawyers began turning over rocks closer to home, however, they discovered what could be called *A Nightmare on Email Street*, a pharmaceutical consultant told Portfolio.com. One of its outside lawyers at Philadelphia-based Pepper Hamilton had mistakenly emailed confidential information on the talks to *Times* reporter Alex Berenson instead of Bradford Berenson, her co-

RELATED CONTENT

From Portfolio

- ▶ A Big Name in Generic Drugs
- ▶ Good News for Pharma Stocks
- ▶ Editor's Letter From Joanne Lipman for May 2007
- ▶ Corporate America Revolts Against Its Lawyers
- ▶ Woolly Bully

News

- ▶ Out of the Gate: Eli Lilly Rises | AP
- ▶ Last Call: Eli Lilly | AP
- ▶ Earnings Preview: Eli Lilly | AP
- ▶ FDA Gives Eli Lilly Drug Priority Review | AP
- ▶ Sector Glance: Big Pharma | AP

[See All Related Content](#)

GET A FREE INDEPENDENT BENCHMARK ANALYSIS.

[GET STARTED](#)

ALSO IN PORTFOLIO.COM

Broker to the Stars
Mauricio Umansky, a.k.a. Paris Hilton's uncle, caters to the celebrity crowd.

Landing in the Rough
The Donald wants to build Europe's largest golf resort.

Lady Sings the News
The new (and only) woman on Rupert Murdoch's board is a 27-year-old fledgling opera diva.

Internet 100%

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.

BlackBerry Reveals Bank's Secrets

Kim Zetter  08.25.03 | 2:00 AM

The eBay ad read "BlackBerry RIM sold AS IS!" So Eugene Sacks (not his real name), a Seattle computer consultant who always wanted one of the pager-size devices to check his e-mail, sent in a bid. For just \$15.50, he bought the wireless device with 4 MB of memory.

The BlackBerry didn't come with a cable, syncing station, software or a manual. But it did come with something even more valuable: a trove of corporate data.

After popping a battery into the BlackBerry's back panel, Sacks discovered a few things the previous owner wouldn't have wanted him to see -- more than 200 internal company e-mails from financial services firm [Morgan Stanley](#) and a database of more than 1,000 names, job titles (from vice presidents to managing directors), e-mail addresses and phone numbers (some of them home numbers) for Morgan Stanley executives worldwide.

It was all there to read, Sacks said, the minute he turned on the device.

The seller, who asked to remain anonymous, was a former vice president of mergers and acquisitions for Morgan Stanley who'd left the company months earlier.

Johnson & Dynes:
Inadvertent Leakage

They examined data that was published
by accident to a P2P Network. This data
is still available ;-)



Definition of Key Concepts

DLP term

Data Loss Prevention

Data Leakage Prevention

Extrusion Prevention

Content Monitoring and Filtering

Data Loss Protection

...

Referring to Rich Mogull, DLP suites are

**products that,
based on central policies,
identify,
monitor,
and protect
data at rest,
in motion,
and in use,
through deep content analysis.**

Leakage

Using the case studies, the following definition explains the term *leakage* in more detail

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

Evaluating DLP Suites

How to evaluate a DLP suite?

“Find weaknesses in DLP [suites]”

But: What are weaknesses in terms of DLP?

- Buffer overflows in endpoint agents?
- SQL Injections in the Webinterface?
- Format string attacks on parsers?

Three main questions

- Is accidental leakage still possible?
- Is it possible to subvert the solution?
- Are there any design flaws?



DLP Test Cases

Test cases – Identify

Are all methods to match data properly working?

- RegEx
- (Cyclic) Hashing
- ...

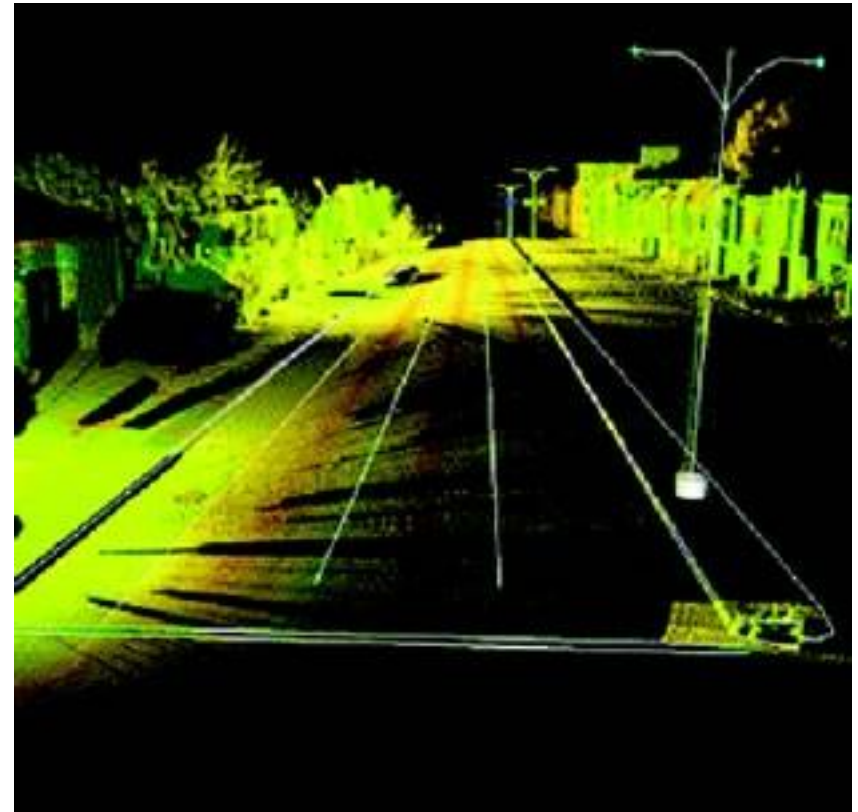
Are all file extensions handled properly?

Are unknown data structures handled properly?

Is encrypted data handled properly?

Test cases – Monitoring

- Are all removable devices (USB, floppy disc, CD) monitored properly?
- Are all file systems monitored properly, including all special functionalities?
- Are all network protocols (Layer 2/3/4) handled properly?
- Are all intercepting network devices monitored properly?
- Is there a possibility to decrypt files using an enterprise encryption system?



Test cases – Reacting

Is sensitive data blocked?

Are all incidents reported properly?

Are there reaction or blocking rules? Allow reaction rules race conditions?

Is there a firewall/proxy integration to block network connections?

Test cases – Design

Is all sensitive traffic encrypted?

Can vulnerabilities be easily found using simple vulnerability assessment methods?

Are all access rights set properly?

Evaluation

Evaluated Solutions

Focus on removable storage media

McAfee Host Data Loss Prevention

- Formerly Reconnex
- Quite new product
- Integrates perfectly in AV/ePO landscape

Websense Data Security Suite

- One of the market leading products
- Stand alone product



Result overview

Test	McAfee	Websense
Textfile/Basic recognition	Green	Green
Filename	Red	Green
PDF	Green	Green
Word/Excel embedment	Green	Green
Compression	Green	Green
Unknown MIME Type	Red	Red
Metadata	Red	Red
NTFS Alternate Data Stream	Green	Green
Third Party Filesystems	Green	Green
Multiple partitions	Red	Green
Secure reaction	Red	Green
Encryption	Red	Red
Fuzzing	Green	Green
Huge files	Red	Red

Test of basic functionality

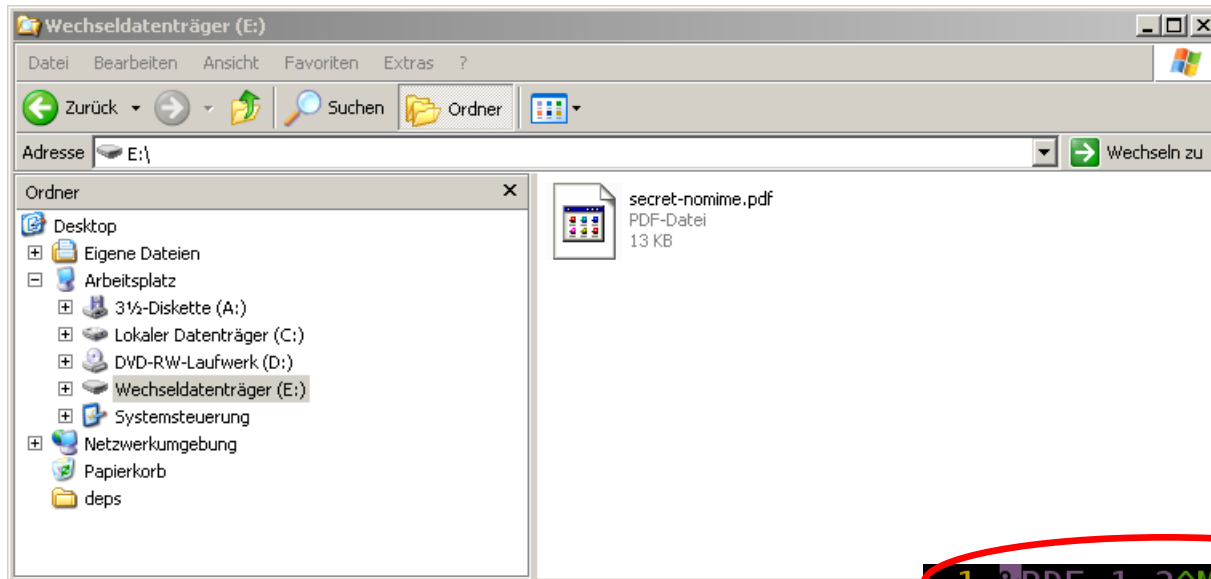
The screenshot displays a security application window titled "Reaction Rules" with a table containing the following information:

Name	Tags	Reactions	Severity	Status
S	secret	Content Based Tag Monitor (Online, Offline), Store Evidence (Online, Offline), Notify User (Online, Offline), Block (Online, Offline)	Critical	Enabled

Below the application window, a Windows desktop environment is visible. It includes:

- A text editor window titled "test.txt - Editor" containing the text "SECRET".
- A Windows Explorer window titled "Wechseldatenträger (E:)" showing the file "test.txt" (Textdokument, 1 KB) in the root directory of the E: drive.
- A taskbar at the bottom with a "test.txt" icon.
- A notification area in the bottom right corner with a red header "McAfee Data Loss Prevention" and a message: "Removable Storage was blocked: e:\test.txt". It includes a link "In Quarantäneordner" and a button "Freigabecode eingeben".

Results: MIME type



```
1 %PDF-1.3^M%âãÏÓ
2 1 0 obj
3 <<
4 /Creator (Canon )
5 /CreationDate (D:20070720103530+01'00')
6 /Producer ( )
7 >>
8 endobj
```

Results: Metadata

The screenshot shows a Windows XP desktop environment. On the left, a file explorer window is open to the E:\ drive, displaying a file named 'exif.png' with a size of 803 KB and a type of 'PNG-Bild'. The status bar at the bottom of the window indicates '1 Objekt(e)' and '802 KB'.

Overlaid on the right side of the file explorer is the 'Image Properties' dialog box for the file 'test.png-1'. The 'Comment' tab is selected, showing the text 'SECRET'. The dialog box includes 'Properties', 'Color Profile', and 'Comment' tabs, and 'Help' and 'Close' buttons at the bottom.

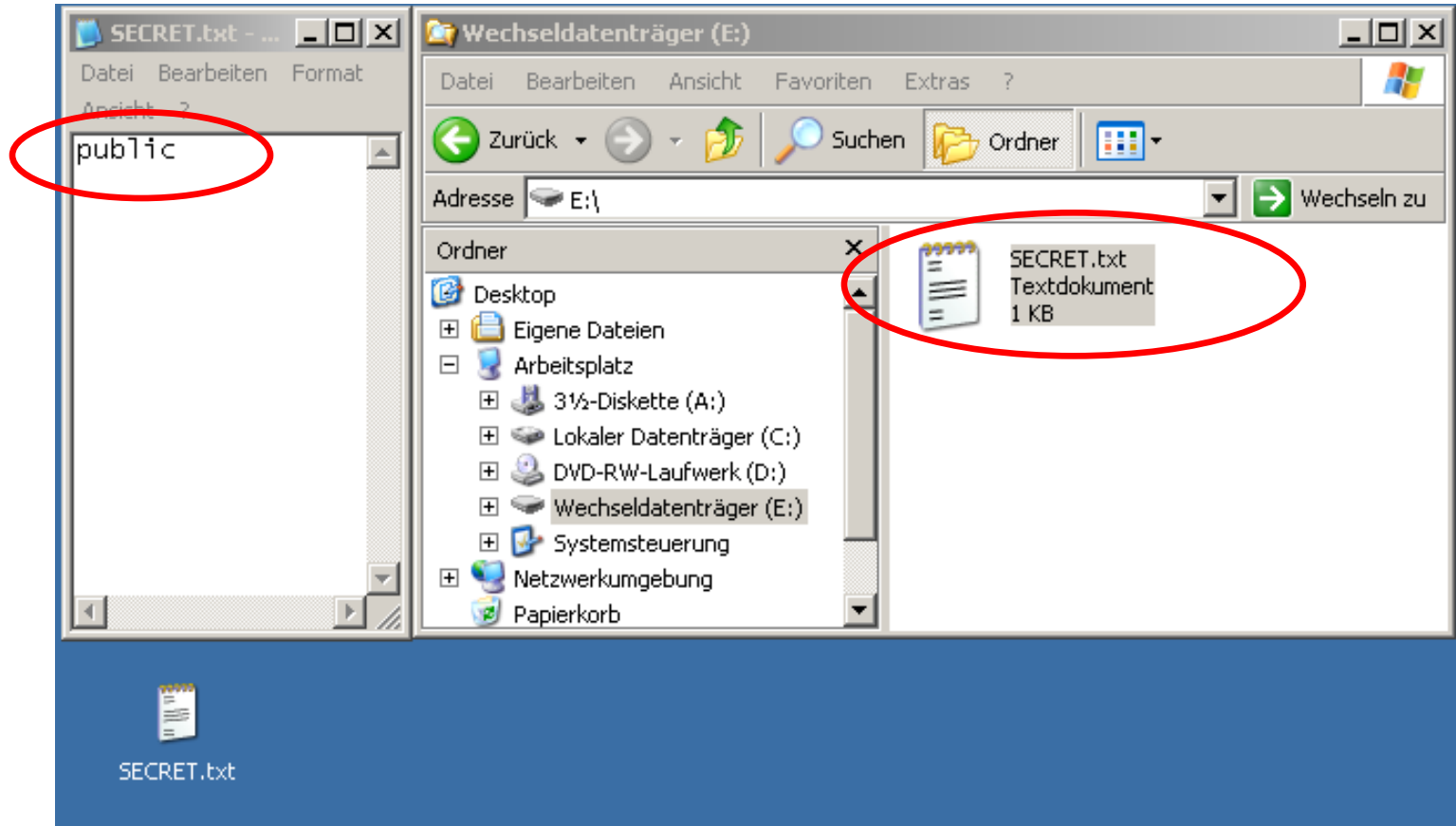
Ordner	Name	Größe	Typ	Geändert am
E:\	exif.png	803 KB	PNG-Bild	11.04.2009 18:46

Image Properties
test.png-1

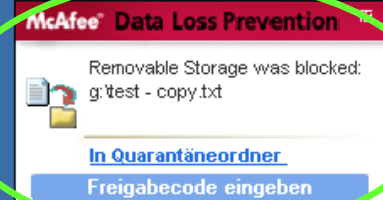
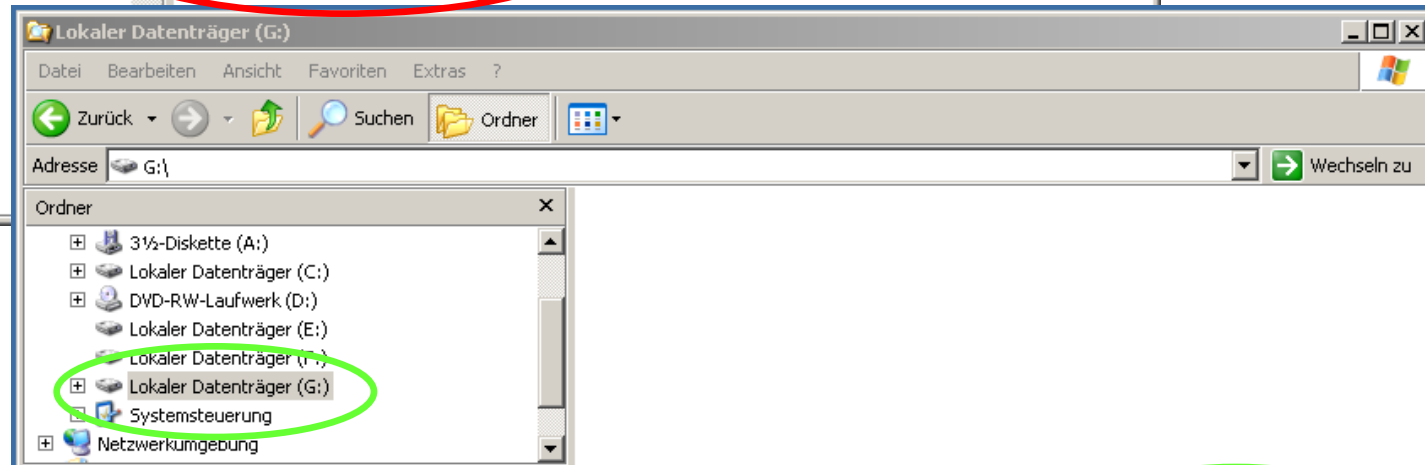
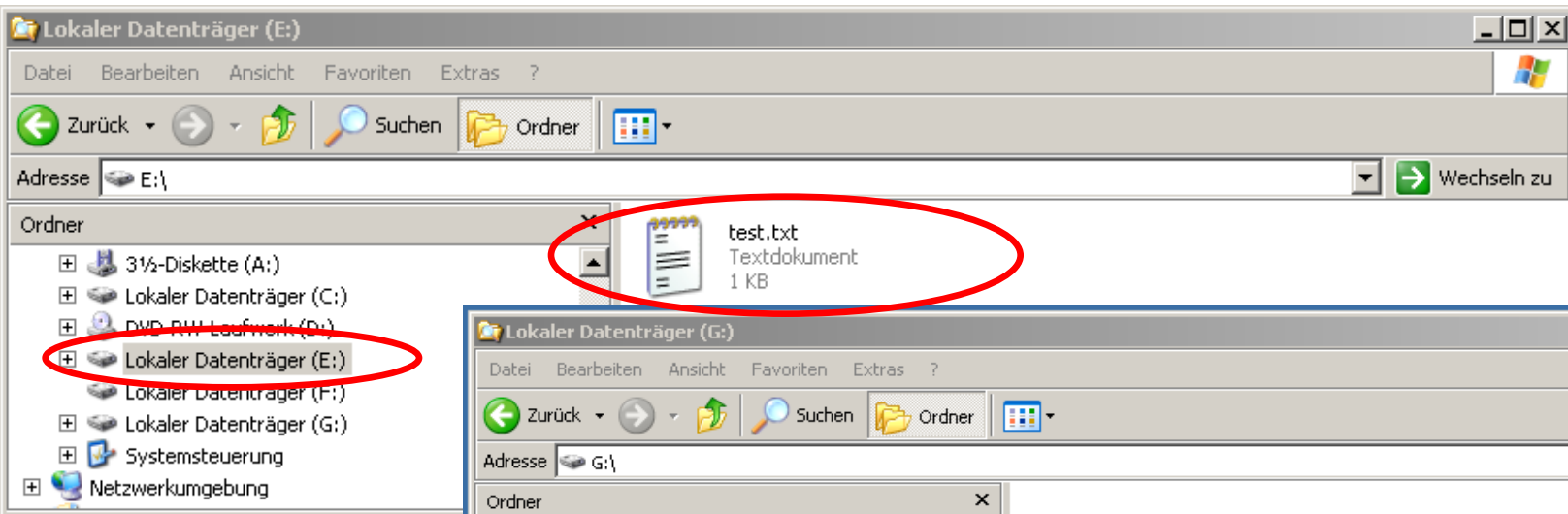
Properties | Color Profile | **Comment**

SECRET

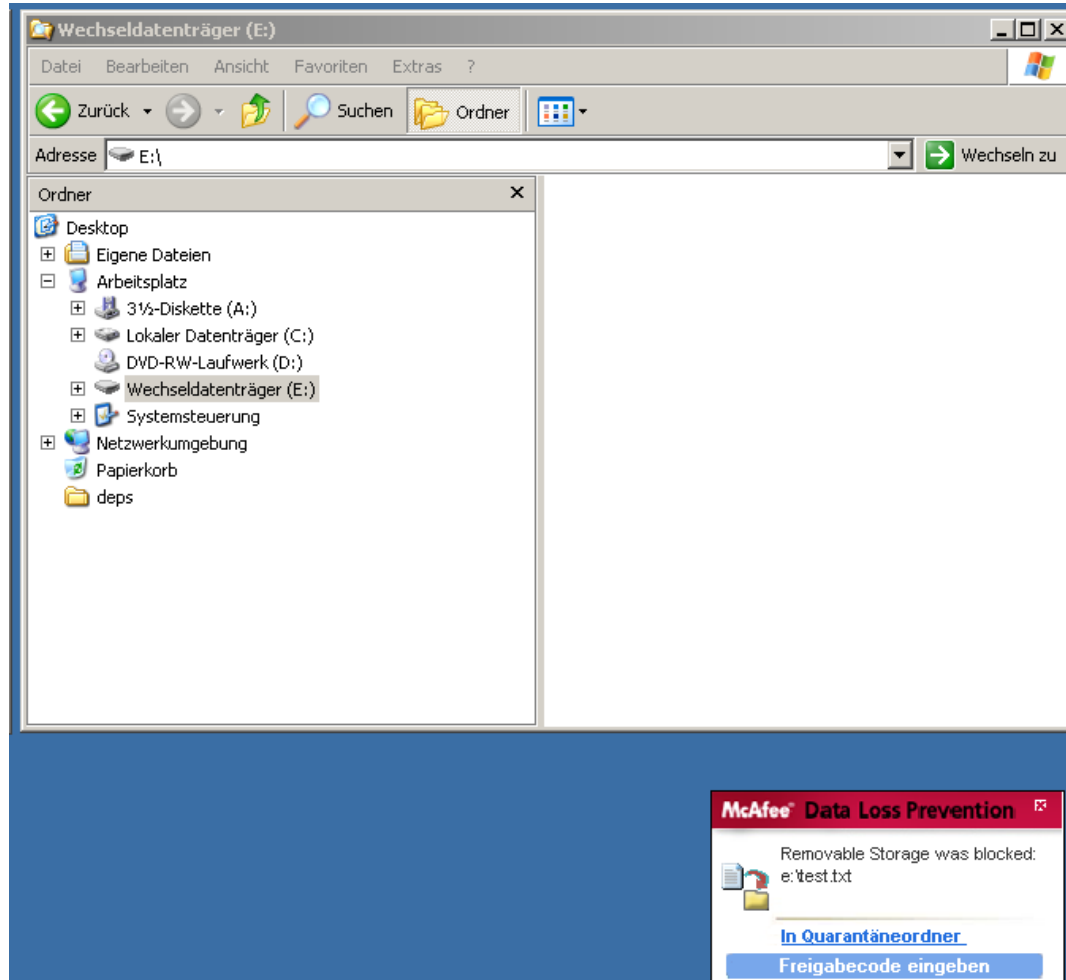
Help Close



McAfee: Multiple partitions



McAfee: Secure reaction



```
File Edit View Terminal Go Help
bender ~ # xxd /dev/fd0 | grep -i secret
0004200: 5345 4352 4554 5345 4352 4554 5345 4352  SECRETSECRETSECR
█
```

```

Shell - Konsole <3>
Tue Apr 14 17:53:11 2009
TCP 172.16.12.85:1189 --> 172.16.12.80:443 | P
CPS_CLIENT5614743444823494669|xp-template|N/A|Incident|..?... "cA..t6XV@.....
.....E.n.d.P.o.i.n.t. .O.p.e.r.a.t.i.o.n.....I.....h.3r.....
...A.c.t.i.v.e.U.s.e.r.....X.P.-.T.E.M.P.L.A.T.E.\.e.r.n.w.....o.p.e.r.a.t.i
.o.n.T.y.p.e.....5.....x.p.-.t.e.m.p.l.a.t.e.....X.P.-.T.E.M.P
.L.A.T.E.\.e.r.n.w.....S.-.1.-.5.-.2.1.-.1.2.2.0.9.4.5.6.6.2.-.1.7.0.8.5.3
.7.7.6.8.-.8.3.9.5.2.2.1.1.5.-.1.0.0.3... ..b...C.:.\.W.I.N.D.O.W.S.\.E.X
.P.L.O.R.E.R..E.X.E.|.%M.i.c.r.o.s.o.f.t..C.o.r.p.o.r.a.t.i.o.n.|.%W.i.n.d.o
.w.s..E.x.p.l.o.r.e.r.|.%B.e.t.r.i.e.b.s.s.y.s.t.e.m..M.i.c.r.o.s.o.f.t...W
.i.n.d.o.w.....U.S.B.0.6.0.7.A..F.l.a.s.h..D.i.s.k.....
.....C.P.S._D.E.V.I.C.E._S.T.O.R.A.G.E._R.E.M.O.V.A.B.L.E.....cX
.....M.e.m.o.r.y.....S.E.C.R.E.T.....d.e.s.t.F.i.l.e.N.a.m
.e.....E.:.\.t.e.s.t..t.x.t...4...C.:.\.D.o.k.u.m.e.n.t.e..u.n.d..E.i.n.s.t
.e.l.l.u.n.g.e.n.\.e.r.n.w.\.D.e.s.k.t.o.p.\.t.e.s.t..t.x.t.....
Tue Apr 14 17:53:11 2009
TCP 172.16.12.85:1189 --> 172.16.12.80:443 | P
.....@NO.....4...C.:.\.D.o.k.u.m.e.n.t.e..u.n.d..E.i.n.s.t.e.l
.l.u.n.g.e.n.\.e.r.n.w.\.D.e.s.k.t.o.p.\.t.e.s.t..t.x.t...t.X.....s.e.c.r.e
.t.....C.o.n.f.i.d.e.n.t.i.a.l.....S.E.C.R.E.T.....

```

Evaluation summary

Test	McAfee	Websense
Textfile/Basic recognition	Green	Green
Filename	Red	Green
PDF	Green	Green
Word/Excel embedment	Green	Green
Compression	Green	Green
Unknown MIME Type	Red	Red
Metadata	Red	Red
NTFS Alternate Data Stream	Green	Green
Third Party Filesystems	Green	Green
Multiple partitions	Red	Green
Secure reaction	Red	Green
Encryption	Red	Red
Fuzzing	Green	Green
Huge files	Red	Red

Further work

Evaluation of more DLP solutions

Evaluation in depth: Network & discovery
functionality

Vulnerability assessment

- It's very likely that there are some ;-)

Creation of a DLP checklist

- *Questions to ask your DLP vendor*

Summary

Both evaluated solutions contained vulnerabilities

- It's all about risk
- Vendors did not react for a very long time

Deployment will very likely cause lots of problems in most environments

- Missing information classification
- Missing awareness of employees
- Missing infrastructure to apply such a huge solution in a safe way

Questions!



Thank you for your attention!

2010
ISSE

