



Live Hacking

06.03.2015

Martin Wundram
DigiTrace GmbH

Ministerium für Wirtschaft, Energie,
Industrie, Mittelstand und Handwerk
des Landes Nordrhein-Westfalen



Agenda (30 Minuten inkl. Fragezeit/Diskussion)



- I. Begrüßung
- II. Storytelling
- III. Live Hacking
- IV. Diskussion

Vortragsort Essen, 06.03.2015



Begrüßung



Über mich

- Martin Wundram
- Diplom-Wirtschaftsinformatiker (Universität zu Köln)
- Von der IHK zu Köln öffentlich bestellter und vereidigter Sachverständiger für Systeme und Anwendungen der Informationsverarbeitung, insbesondere IT-Sicherheit und IT-Forensik
- Geschäftsführer DigiTrace GmbH, TronicGuard GmbH
- Standort Köln
 - 6 Personen im Team
 - Kunden von KMU bis DAX + Behörden



Vortragsort Essen, 06.03.2015



Begrüßung



Meine Einschätzung

- Ein Statement zu **IT-Sicherheit**
 - Mittlerweile ist die Informationssicherheit eines Jeden umfassend, nachhaltig und konkret durch Angriffe und Pannen bedroht. Gegenmaßnahmen können helfen und werden dringend benötigt; insbesondere Know-How und Problembewusstsein beim Anwender



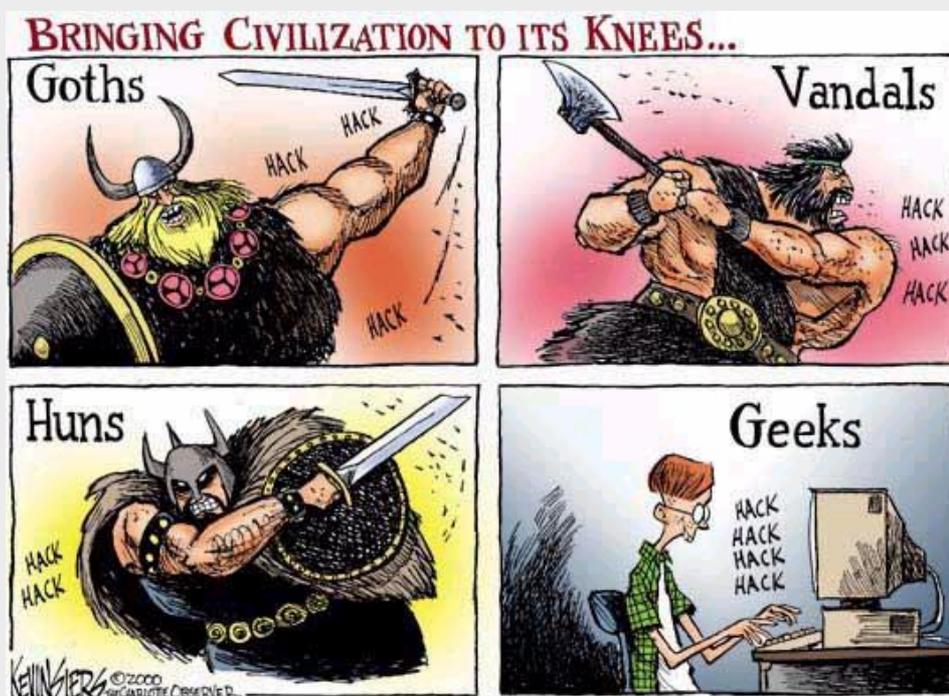
Vortragort Essen, 06.03.2015



Begrüßung



Begrüßung



Vortragsort Essen, 06.03.2015

Begrüßung



Has your credit card number been **STOLEN** on the Internet?

card number

expires

Vortragsort Essen, 06.03.2015



Begrüßung

Fast täglich neue Meldungen

Spionagesoftware-Firma Gamma: Hacker veröffentlicht 40-Gigabyte-Datensatz

Das Unternehmen Gamma International verkauft Hacker-Werkzeuge an Regierungen in aller Welt. Nun ist die Firma angeblich selbst zum Opfer eines Hackers geworden - der in großem Stil Unternehmensdaten veröffentlicht.

Nachrichten (2 ungelesen)

Chrome: Update schließt 159 Sicherheitslücken

"Shellshock": Schwere Sicherheitslücke bedroht Macs und Linux-Rechner

SPIEGEL ONLINE - 25.09.2014

Ohne Funktion: Erfolgreiche Virenschutz-App für Android war ein Fake

einem Uraltprogramm, das auf vielen Unix- und Linux-Rechnern deren Sicherheit. Experten sprechen von Ausmaßen wie beim Rechner sind betroffen. Es gibt einen einfachen Selbsttest.



Gefährlich: Botnetz mit 18.000 befallenen Macs entdeckt

AndroneWS - vor 1 Stunde

Apples Macs hatten bis dato ihren Microsoft-PC-Kollegen eines voraus – ein Viren- und Trojaner-Schutz war eigentlich gar nicht nötig, hieß es ...



Noch 300.000 Server betroffen: Sicherheitslücke Heartbleed nimmt kein Ende

SPIEGEL ONLINE - 23.06.2014

Drei Monate nach Bekanntwerden sind 300.000 Internet-Server noch immer von der Heartbleed-Sicherheitslücke betroffen. Nach Meinung eines Sicherheitsexperten wird sich das auch in den nächsten zehn Jahren kaum ändern. mehr... [Forum]



AUF DER FLUCHT

John McAfee mit iPhone-Geolocation geortet

Der IT-Gründer John McAfee hat sich auf der Flucht vor Journalisten mit dem iPhone fotografieren lassen, und die Bilddaten verriet seinen geheimen Aufenthaltsort. McAfee verbreitete in seinem Blog, er habe die EXIF-Daten in dem Bild manipuliert, und löschte die Lüge dann schnell wieder.

04.12.2012 36 Kommentare



Cyberattacke auf JPMorgan: über 83 Millionen Konten gefährdet

T-Online - 02.10.2014

Betroffen seien die Konten von 76 Millionen Haushalten und sieben Millionen Firmen, teilte das Unternehmen seinen Kunden und der ... JP Morgan: Hackerangriff betraf 76 Millionen Haushalte Spiegel Online - 02.10.2014

Begrüßung

Ransomware

US-Polizisten zahlen Lösegeld für ihre Daten



Eine amerikanische Polizeistation ist Opfer eines Lösegeld-Trojaners geworden. Doch statt ruhig zu bleiben, zahlten die Polizisten rund 600 Dollar an die Erpresser. Dabei hätte es vielleicht eine viel einfachere und preiswertere Lösung gegeben. **mehr...** [Forum]

Quelle: <http://www.spiegel.de/netzwelt/> (abgerufen 24.02.2015)

HBGary Federal vs. Anonymous

1. Der CEO Aaron Barr erklärt öffentlich, er habe **Anonymous infiltriert** und Identitäten enttarnt und wolle die **Informationen dem FBI übergeben** (ein Blog-Beitrag und eine Pressemeldung waren bereits verfasst).
2. Er mailt einer PR-Mitarbeiterin: „As 1337 as these guys are supposed to be they don't get it. I have pwned them! :)“
3. Schon einen Tag nach der öffentlichen Ankündigung holt Anonymous zum **Gegenschlag** aus.

Quelle z.B. Heise: <http://www.heise.de/ct/artikel/Ausgelacht-1195082.html>

HBGary Federal vs. Anonymous

Der Gegenschlag:

1. Aus dem selbst entwickelten CMS konnten per **SQL-Injection** die Passwort-Hashes der Accounts entwendet werden.
2. Diese Hashes waren sehr unsicher und die Passwörter konnten daraus abgeleitet werden.
3. HBGary-Mitarbeiter verwendeten diese Passwörter für mehrere Accounts (E-Mail, Twitter, Linked-In, System-Accounts, ...).
4. So war der Zugriff auf support.hbgary.com möglich, einem ungepatchten Linux-Server → Zugriff auf mehrere GB Backup- und Forschungsdaten.
5. Zugriff auf Google-Apps → Änderung der Passwörter anderer Mitarbeiter.

Quelle z.B. Heise: <http://www.heise.de/ct/artikel/Ausgelacht-1195082.html>

HBGary Federal vs. Anonymous

Der Gegenschlag (Fortsetzung):

1. In dem Mail-Account von Greg Hوجلund befand sich das Superuser-Passwort für den Webserver www.rootkit.com.
2. Über den Mail-Account von Greg Hوجلund dann ein **Social Engineering-Angriff** auf einen Administrator des Unternehmens → Dieser schaltete die Firewall ab, was den Abgriff von tausenden Benutzerkontendaten von www.rootkit.com ermöglichte.
3. Anonymous veröffentlichte anschließend eine Vielzahl vertraulicher Informationen:
 1. Über **60.000 E-Mails** aus den HBGary-Postfächern.
 2. Alle [rootkit.com](http://www.rootkit.com)-Passwort-Hashes.
 3. Informationen bzgl. Wikileaks, **Bank of America, U.S. Chamber of Commerce**.

Quelle z.B. Heise: <http://www.heise.de/ct/artikel/Ausgelacht-1195082.html>

Storytelling

HBGary Federal vs. Anonymous



aaronbarr

Today we taught everyone a lesson. When we actually decide to bite back against those who try to bring us down, we bite back hard. #gameover

23 minutes ago via web

Here's my address:

about 1 hour ago via web

Storytelling

rootkit.com cleartext passwords

On February 6, 2011, as part of their [attack on HBGary](#), the Anonymous group [social engineered](#) administrator of rootkit.com, Jussi Jaakonaho, to gain root access to rootkit.com. The entire MySQL database backup was then released by Anonymous and announced using HBGary's CEO Twitter account, [@aaronbarr](#): *Sup, here's rootkit.com MySQL Backup http://stfu.cc/rootkit.com_mysqlBackup_02_06_11.gz #hbgary #rootkit #anonymous*. The table below is the list of accounts found in rootkit.com MySQL database backup with passwords in cleartext.

JTR is used to translate the password to cleartext_password. The list with id:cleartext_password combination is available in [plaintext format](#). Most of the passwords were successfully acquired by feeding a [password dictionary](#) to JTR and the rest are being acquired by using JTR incremental mode. By randomly putting the passwords to test, many appear to be reused by the same user elsewhere on sites presumably of lower value to the user, e.g. Facebook, Twitter, forum sites, secondary email accounts, etc. If your account or account of someone you know appears in the list below, we urge you to take an action to change the password immediately if it is used elsewhere.

[Online-Kredit in 2 Min.](#) Kredit auch ohne Schufa möglich. Sofort-Zusage sichern... MAXDA.de/Kreditantrag

[Gold Support Customer?](#) Get Platinum database support for your LAMP apps at Gold prices. www.skyql.com/en/MySt

[Send Direct Email](#) Campaigns right from your PC. No recurring fees. Free download. www.ArialSoftware.com



Tweet 137 Gefällt mir 48

Ads by Google

search email clear

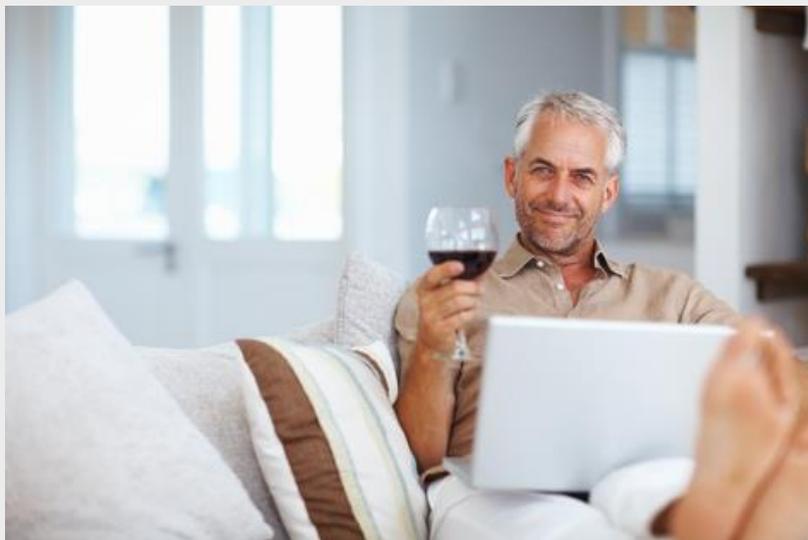
Page 1 of 90. next **44504 accounts**

id	password	name	email	cleartext_password
333	fdb99870961edb29f88241bbd99d890		charlesw@n	foofoo
516	b9ea618e2c434af00017bd45b5a7cb48		spamjail@m	1satriani
594	fcea920f7412b5da7be0cf42b89c93759		testing2468	1234567
796	74ed65aeddf3b5ad672d9c30def57f3d		zig@	datalfie
1171	14a7cb10eb0fbc01963990945e66eb8b		minjack.t	mjloveno
1193	ed453a39fd64a5b4f3422281a3cb5ba4		netmania	adik1981
1472	613e3606eb366eaa2c7c831ab0afd4c		mauro.pa	mang1729
1817	795fd4e170d0a5cf013ef8af5b8e31e2		twoken@	19790809
1866	3f8cb308e807fdf213f43d08eac6df2b		nabu@be	abomb001
2820	8ec5af667b7be97ddeb18db02882607d		adminis@	141421
3718	c25292cec7118591564f25784250225c		tsm@	pah67590
3989	4abc4e1dff4cfb3d781455b669ea7a51		drage	kokolino
4391	9dae8b007b5d460c606fac70b701d44		willia	guru11
4570	9fd8301ac24fb88e65d9d7cd1dd1b1ec	Kelsey Leary	kelsey@hbgary.com	butterfly
4856	a2759ccd00aa041f4ba9d5ea7c4ae5f2		remember	bolivar
5115	6e32a847a493cf724df9772185e2e9fa		leighton.s	l9s8d78
5514	d16b6d126b09ac17a4c37a5e503480a1		kodmaker	cryptman
5817	cbdb7e2b1ed566ceb796af2df07205a3		plsharma	bond007
5838	b2f3f9771f1e9e72fc244d49adfb0142		coolsume	801225
6000	ca1e1111111111111111111111111111			2011 © Dazzelep

Live Hacking



Live-Demonstration ausgewählter (aktueller) Angriffswege



Vortragsort Essen, 06.03.2015



Live Hacking - gezeigte Angriffe



- **Webseiten** der „Crank Steuerberatung“ hacken (XSS, SQL-Inject, CSRF)
- Mit Schadcode (**trojanisiertes Programm**) wichtige Daten verschlüsseln und **Lösegeld** erpressen
- Ein Bit „verdrehen“ und Computer in die Falle locken

Vortragort Essen, 06.03.2015



Webseiten der “Crank Steuerberatung”

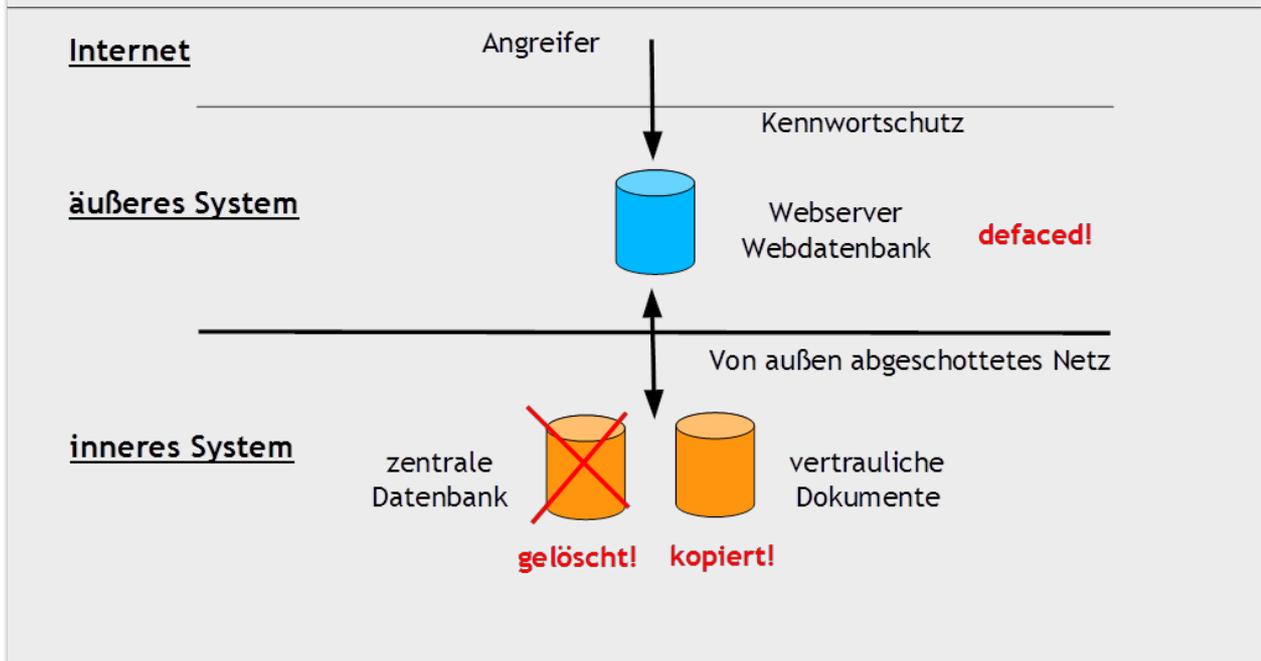


Angriffs-Szenario

- Ein ehemaliger Mitarbeiter der Crank Steuerberatung Ltd., der vor kurzem außerordentlich gekündigt wurde und nicht mehr dort tätig ist, sinnt auf Rache.
- Sein Ziel ist, über das Internet in die geschützte Unternehmens-IT einzudringen, vertrauliche Dokumente abzugreifen und das Unternehmen durch Löschung der zentralen Datenbank und Änderung der Webseiten nachhaltig zu schädigen.
- Er kennt die Unternehmens-IT und Gepflogenheiten, hat aber keine aktuellen Kennwörter mehr.
- **Wie geht er technisch vor?**

Webseiten der "Crank Steuerberatung"

Das Vorgehen



Webseiten der “Crank Steuerberatung”



Angriffs-Technik

- **Äußeres System:**
 - SQL-Injection und
 - Persistent XSS
- **Inneres System:**
 - Cross Site Request Forgery (CSRF),
automatische Schadaktionen

Webseiten der "Crank Steuerberatung"



Der Angriff

Crank Steuerberatung Ltd.



Gebuehren	Services	Beratung	Ihre Vorteile
Home Über uns	Willkommen bei Crank Steuerberatung Ltd., Ihrem Spezialisten für Steuerberatung, Geld Sparen und die sichere Speicherung Ihrer Daten. Bleiben Sie gelassen, lehnen Sie sich zurück, wir übernehmen den unangenehmen Rest. 	 Hotline: 0180 0815	Sonderangebot Sonderangebot Erstberatung ab sofort kostenfrei!

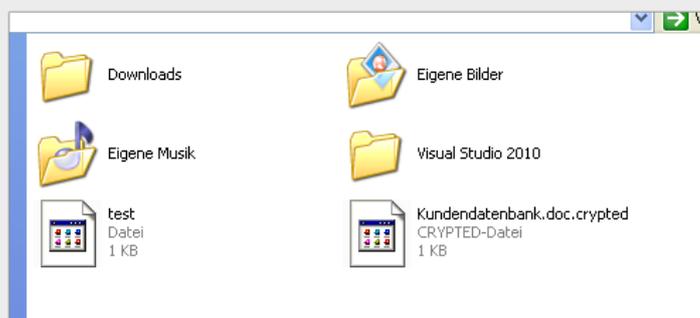
Vortragsort Essen, 06.03.2015



Verschlüsselungstrojaner

Ransomware: Ein Trojaner verschlüsselt wichtige Daten/Angriff

- Durch einen Man-In-The-Middle-Angriff „motiviert“ hat das Opfer einen tollen Taschenrechner heruntergeladen und gleich ausprobiert.
- Dieser Taschenrechner rechnet jedoch krumm...

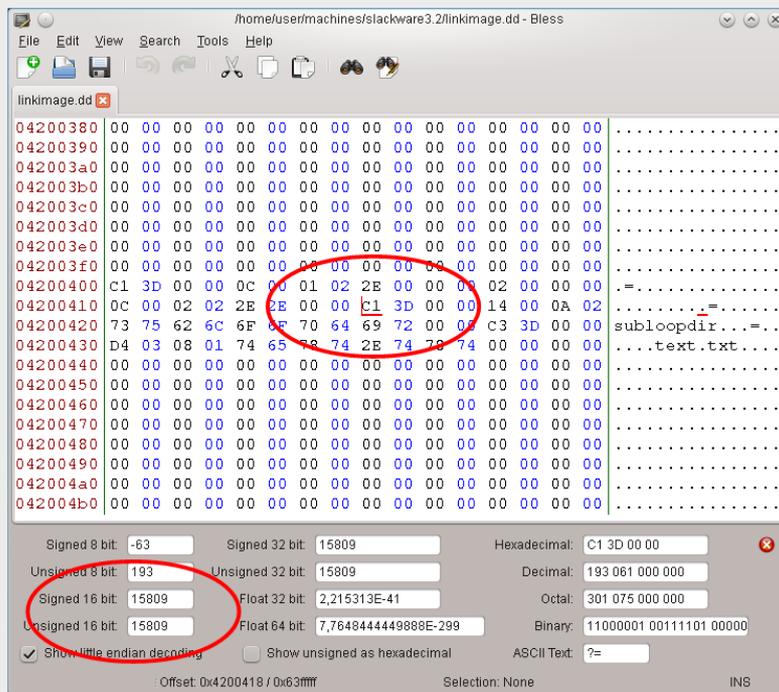


Ransomware: der Schaden

- Alle (wichtigen?) persönlichen Daten sind weg. Für immer. Niemand kann helfen. Es sei denn, man kauft das passende Entschlüsselungsprogramm (oder hat ein Backup)...
- Wichtige Mandantendaten
- Geschäftsdokumente, zu deren sicherer Verwahrung man gesetzlich verpflichtet ist
- Die Diplomarbeit/Dissertation
- ...

Live Hacking: Beispiel für eine "Tretmine"

Verzeichnis-Schleifen



The screenshot shows a hex editor window titled "/home/user/machines/slackware3.2/linkimage.dd - Bless". The main area displays a hex dump of a directory listing. A red circle highlights the hex value `C1 3D 00 00` at offset `04200410`, which corresponds to the directory entry `subloopdir`. Below the hex dump, there is a conversion panel with various input fields. A red circle highlights the `Signed 16 bit` field, which contains the value `15809`. Other fields include `Signed 8 bit` (-63), `Unsigned 8 bit` (193), `Signed 32 bit` (15809), `Unsigned 32 bit` (15809), `Hexadecimal` (C1 3D 00 00), `Decimal` (193 061 000 000), `Octal` (301 075 000 000), `Float 32 bit` (2,215313E-41), `Float 64 bit` (7,7648444449888E-299), `Binary` (11000001 00111101 00000), `ASCII Text` (?=), and `Show little endian decoding` (checked).

Vortragort Essen, 06.03.2015

Live Hacking

„Hacker-Datenbanken“ ShodanHQ und Google

- Suchstring: webcamxp

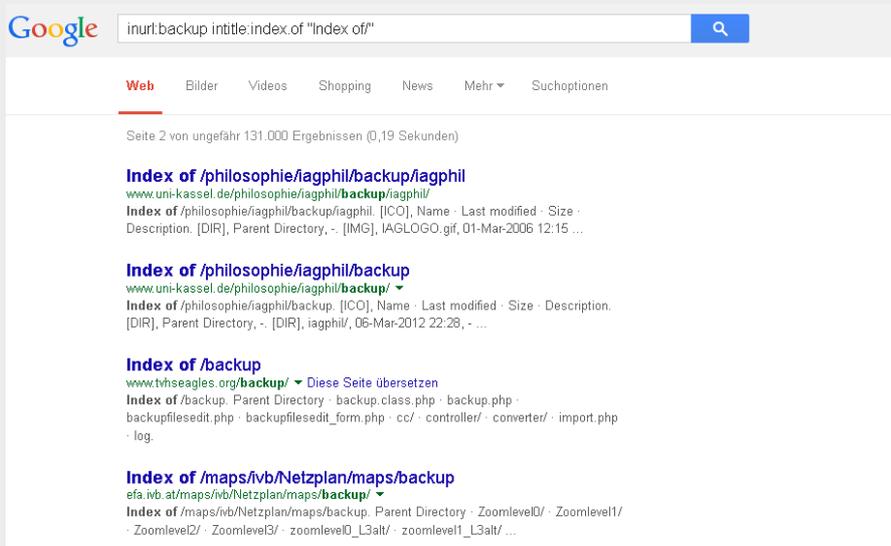


Vortragsort Essen, 06.03.2015

Live Hacking

„Hacker-Datenbanken“ ShodanHQ und Google

- Suchstring: `inurl:backup intitle:index.of "Index of/"`
- Beispiel: `http://www.landkreis-waldshut.de/landkreis-waldshut/fileadmin/user_upload/_temp_/`



Google

Web Bilder Videos Shopping News Mehr ▾ Suchoptionen

Seite 2 von ungefähr 131.000 Ergebnissen (0,19 Sekunden)

Index of /philosophie/iagphil/backup/iagphil
www.uni-kassel.de/philosophie/iagphil/backup/iagphil/
Index of /philosophie/iagphil/backup/iagphil. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, · [IMG], IAGLOGO.gif, 01-Mar-2006 12:15 ...

Index of /philosophie/iagphil/backup
www.uni-kassel.de/philosophie/iagphil/backup/ ▾
Index of /philosophie/iagphil/backup. [ICO], Name · Last modified · Size · Description. [DIR], Parent Directory, · [DIR], iagphil/, 06-Mar-2012 22:28, · ...

Index of /backup
www.tvhseagles.org/backup/ ▾ Diese Seite übersetzen
Index of /backup. Parent Directory · backup.class.php · backup.php · backupfilesedit.php · backupfilesedit_form.php · cc/ · controller/ · converter/ · import.php · log.

Index of /maps/fvb/Netzplan/maps/backup
efa.wb.at/maps/fvb/Netzplan/maps/backup/ ▾
Index of /maps/fvb/Netzplan/maps/backup. Parent Directory · Zoomlevel0/ · Zoomlevel1/ · Zoomlevel2/ · Zoomlevel3/ · zoomlevel_L3alt/ · zoomlevel1_L3alt/ ...

Welche Fragen haben Sie?



Autor:
Martin Wundram / Geschäftsführer

E-Mail:
wundram@digitrace.de

Unternehmen:
DigiTrace GmbH
Zollstockgürtel 59
50969 Köln

Web:
www.digitrace.de



Vielen Dank für Ihre
Aufmerksamkeit!

