nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

Live Hacking

06.03.2015

Martin Wundram
DigiTrace GmbH

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

DigiTrace
Kompetenz in IT-Forensik

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds
für regionale Entwicklung

Agenda (30 Minuten inkl. Fragezeit/Diskussion)

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

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

DigiTrace
Kompetenz in IT-Forensik

Begrüßung

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

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

DigiTrace
Kompetenz in IT-Forensik

Begrüßung

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

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

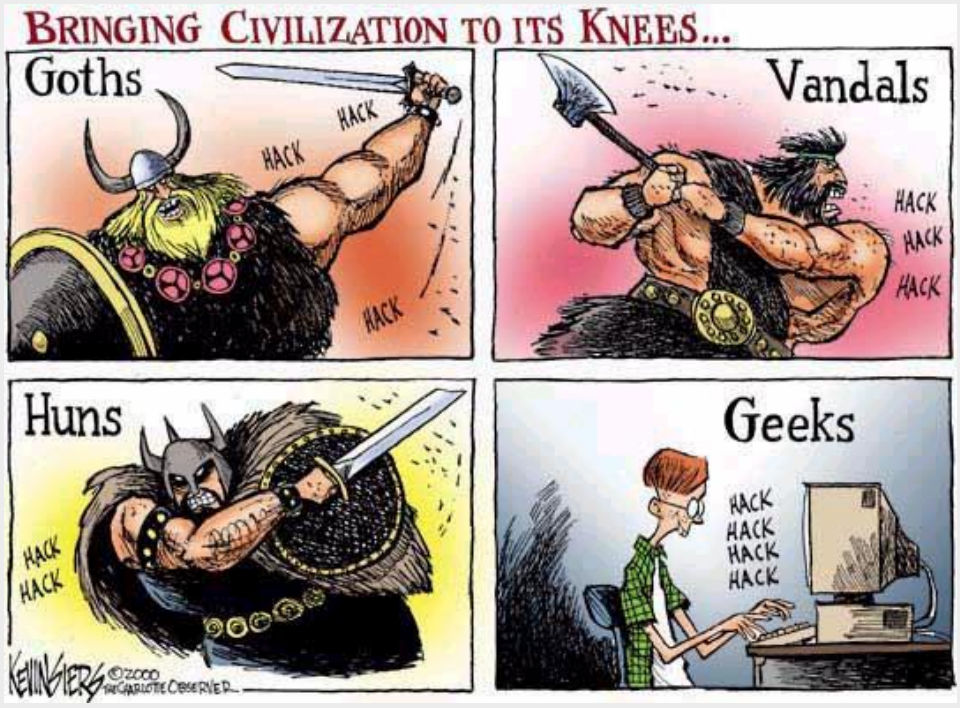
Dipl.-Wirt.-Inf. Martin Wundram
Sachverständiger für Systeme u. Anwendungen der Informationsverarbeitung, insbesondere IT-Sicherheit und IT-Forensik
Von der Industrie- und Handelskammer öffentlich bestellter und vereidigter Sachverständiger

DigiTrace
Kompetenz in IT-Forensik

Begrüßung

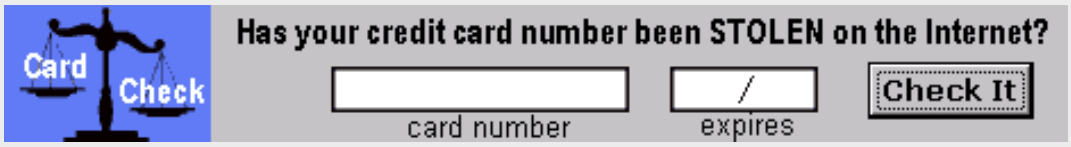

Netzwerk
Sent (2)
1351
bayimg - image: Screens
Lea...
Downlo...
Downlo...
Downlo...
bayimg.com/fa
Firefox hat diese Website daran gehindert, 63 Pop-up-Fenster zu öffnen.
BAYIMG
Free uncensored image hosting

Begrüßung



Vortragsort Essen, 06.03.2015

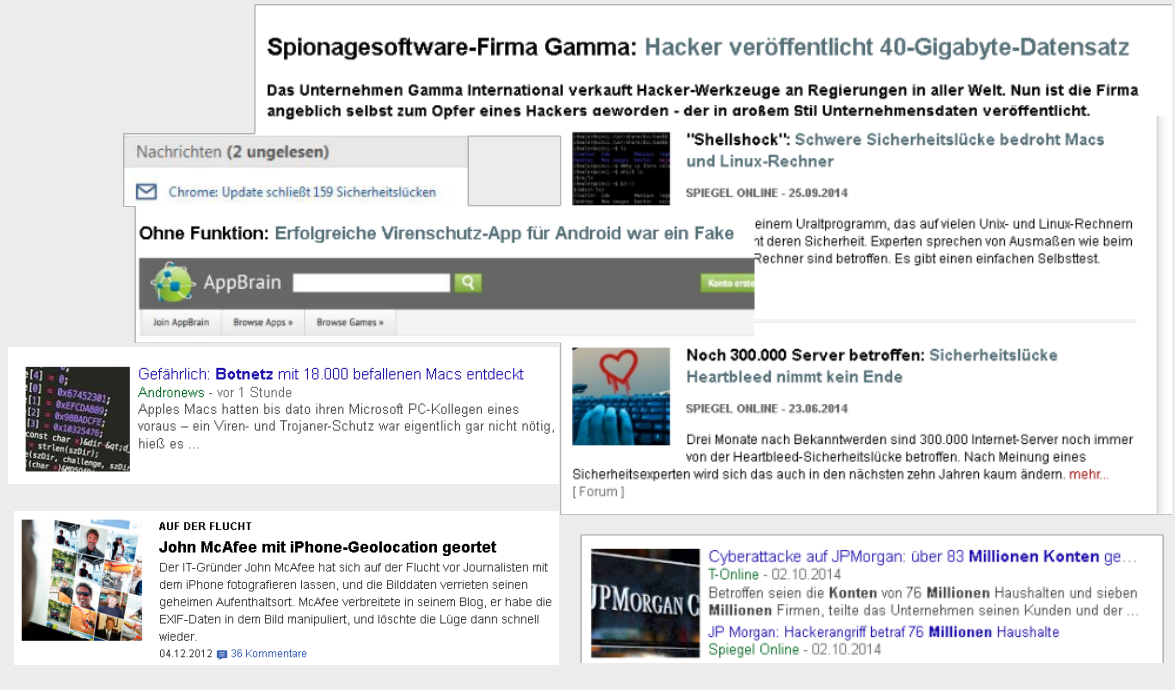
Begrüßung


Card
Check
Has your credit card number been STOLEN on the Internet?
card number
/
expires
Check It

Begrüßung

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

Fast täglich neue Meldungen



Vortragsort Essen, 06.03.2015

DigiTrace
Kompetenz in IT-Forensik

Begrüßung

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

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)

DigiTrace
Kompetenz in IT-Forensik

Storytelling

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

Storytelling

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

Storytelling

HBGary Federal vs. Anonymous

Der Gegenschlag (Fortsetzung):

1. In dem Mail-Account von Greg Hoglund befand sich das Superuser-Passwort für den Webserver www.rootkit.com.
2. Über den Mail-Account von Greg Hoglund 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-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

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

HBGary Federal vs. Anonymous

DigiTrace
Kompetenz in IT-Forensik

Storytelling

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

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.

search email clear

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

id	password	name	email	cleartext_password
333	fdba98970961edb29f88241b9d99d890	[redacted]	charlesw@n[redacted]	foofoo
516	b9ea618e2c434af00017bd45b5a7cb48		spamjail@m[redacted]	1satriani
594	fcea920f7412b5da7be0cf42b8c93759		testing2468[redacted]	1234567
796	74ed65aeddf3b5ad672d9c30def57f3d		zig@[redacted]	datalife
1171	14a7cb10eb0fbc01963990945e66eb8b		minjack.tv[redacted]	mjlovemo
1193	ed453a39fd64a5b4f3422281a3cb5ba4		netmania[redacted]	adik1981
1472	613e3606eb366ecaa2c7c831ab0afd4c		mauro.pa[redacted]	mang1729
1817	795fd4e170d0a5cf013ef8af5b8e31e2		twoken@[redacted]	19790809
1866	3f8cb308e807fdf213f43d08eec6df2b		nobu@be[redacted]	abomb001
2820	8ec5af667b7be97ddeb18db02882607d		adminis@[redacted]	141421
3718	c25292cec7118591564f25784250225c		tsm@[redacted]	pah67590
3989	4abc4e1dff4cfb3d781455b669ea7a51		dragc[redacted]	kokolino
4391	9dae8b007b5d460c6068fac70b701d44		willia[redacted]	guru11
4570	9fd8301ac24fb88e65d9d7cd1dd1b1ec	Kelsey Leavy	kelsey@hbgary.com	butterfly
4856	a2759ccd00aa041f4ba9d5ea7c4ae5f2	[redacted]	remember[redacted]	bolivar
5115	6e32a847a493cf724df9772185e2e9fa		leighton_s[redacted]	l9s8d78
5514	d16b6d126b09ac17a4c37a5e503480a1		kodmaker[redacted]	cryptman
5817	cbdb7e2b1ed566ceb796af2df07205a3		plsharma-[redacted]	bond007
5838	b2f3f9771f1e9e72fc244d49adfb0142		coolsume[redacted]	801225

DigiTrace
Kompetenz in IT-Forensik

Live Hacking

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

Live-Demonstration ausgewählter (aktueller) Angriffswege

Vortragsort Essen, 06.03.2015

DigiTrace
Kompetenz in IT-Forensik

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

Webseiten der “Crank Steuerberatung”

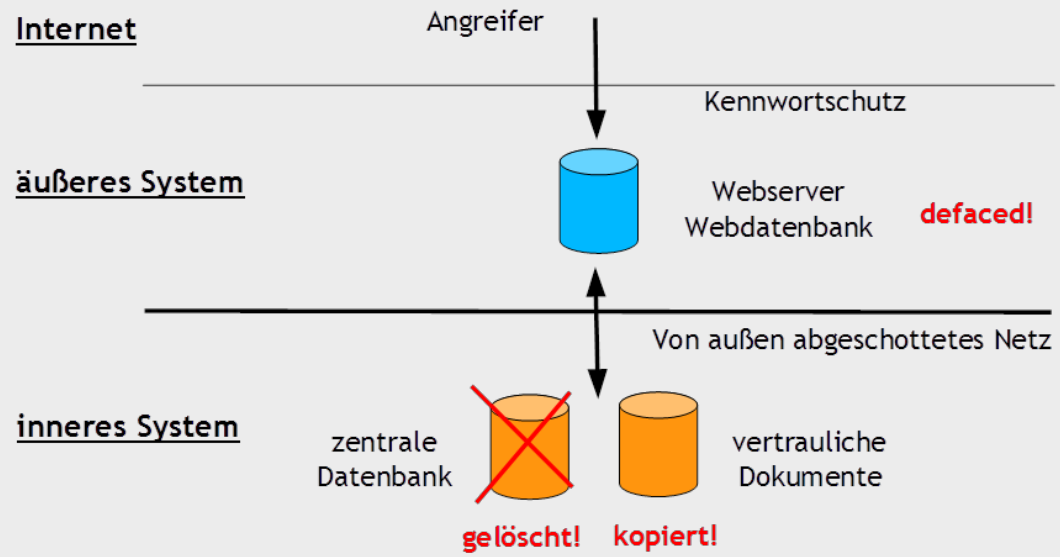
Angriffs-Szenario

- 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”

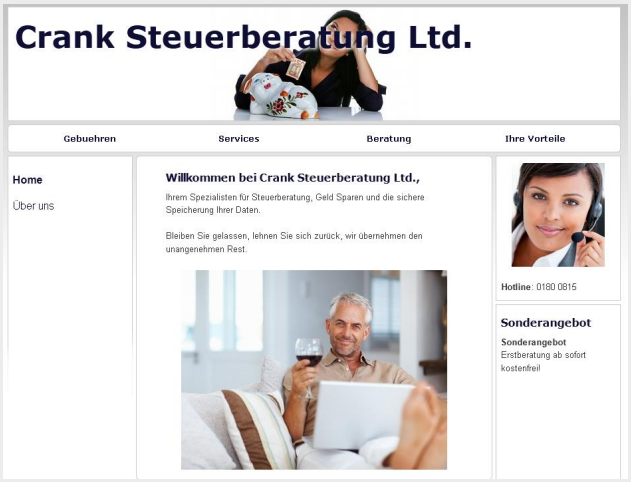
Angriffs-Technik

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

Webseiten der “Crank Steuerberatung”

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

Der Angriff

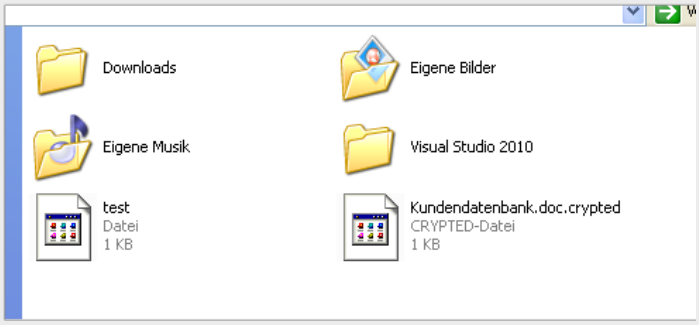


DigiTrace
Kompetenz in IT-Forensik

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…



Live Hacking

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

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)...

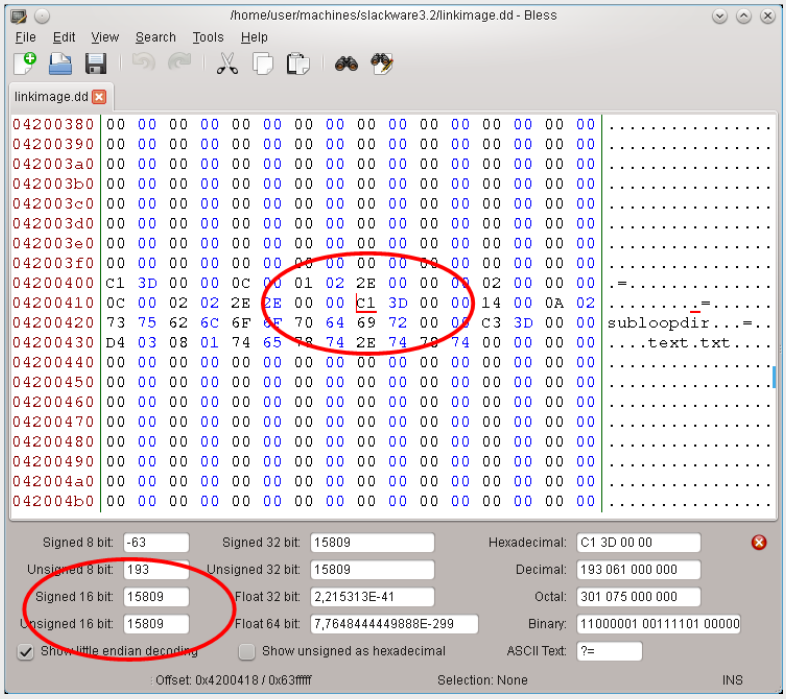
- Wichtige Mandantendaten
- Geschäftsdokumente, zu deren sicherer Verwahrung man gesetzlich verpflichtet ist
- Die Diplomarbeit/Dissertation
- ...

DigiTrace
Kompetenz in IT-Forensik

Live Hacking: Beispiel für eine “Tretmine”

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

Verzeichnis-Schleifen



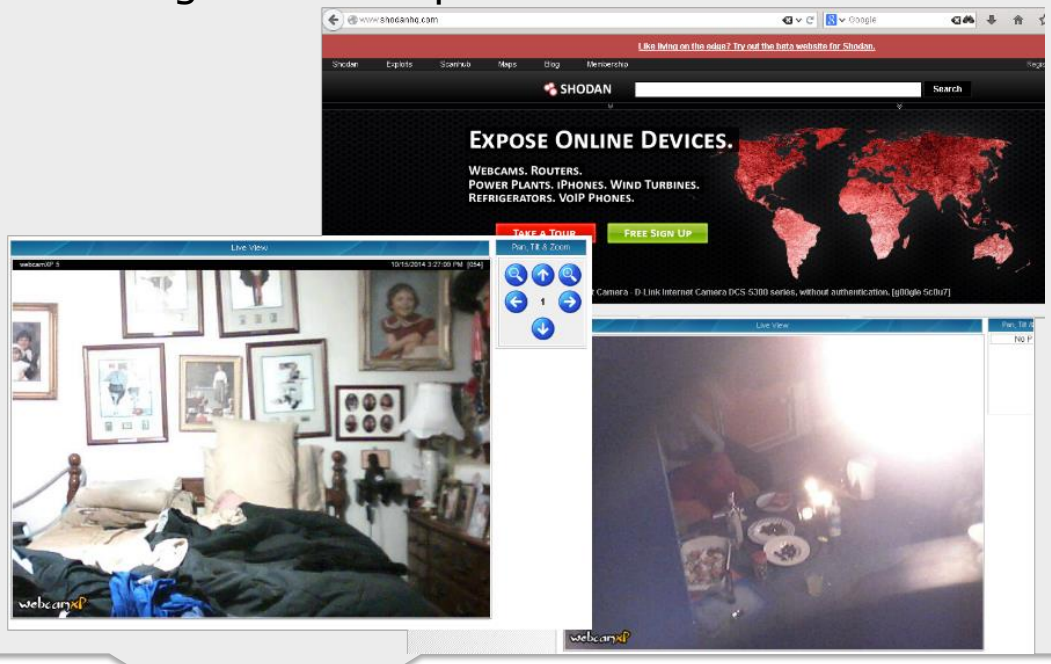
DigiTrace
Kompetenz in IT-Forensik

Live Hacking

nrw-unITS
IT-Sicherheit
Nordrhein-Westfalen

„Hacker-Datenbanken" ShodanHQ und Google

- Suchstring: webcamxp



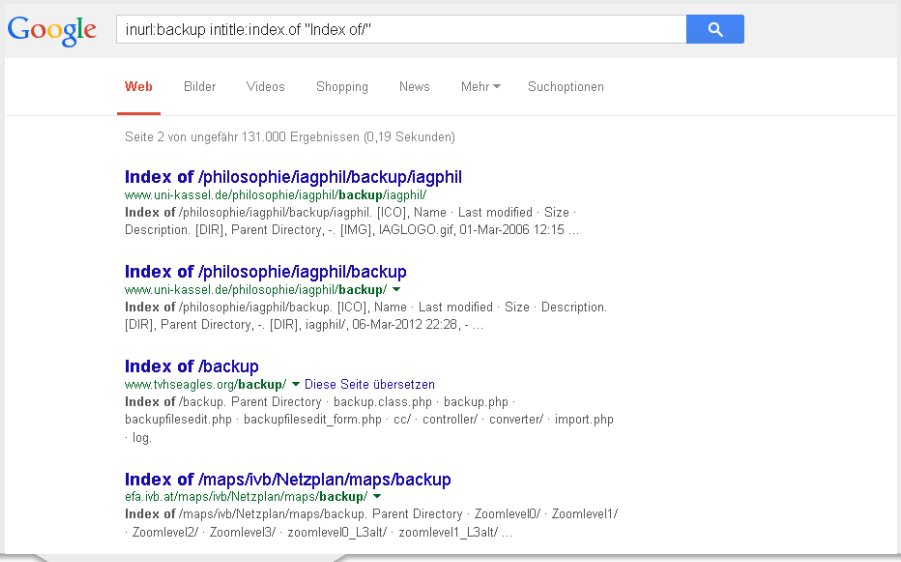
DigiTrace
Kompetenz in IT-Forensik

Live Hacking

nrw-uniTS
IT-Sicherheit
Nordrhein-Westfalen

„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_/



DigiTrace
Kompetenz in IT-Forensik

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!

nrw-uniTS IT-Sicherheit Nordrhein-Westfalen

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

DigiTrace Kompetenz in IT-Forensik

EUROPÄISCHE UNION
Investition in unsere Zukunft
Europäischer Fonds für regionale Entwicklung