IT-Exchange München

IT-Sicherheit und IT-Forensik: Schwerpunkt Web/Internet

Martin G. Wundram
wundram@tronicguard.com


Die Stecker an der Kasse sowie
dem W-Lan Acces Point sind zu
keinem Zeitpunkt
auszustecken!!! Auch nicht zum
Staubsaugen!!!
hem Gruß

Agenda

Inhalte dieser Einheit

1. Vorstellung aktueller und „historischer“ Vorfälle
2. Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken
3. SQL-Injection und andere Fälle
4. Fazit

Ziele des Vortrags

- Vorstellung aktueller und „historischer“ Fälle mit Schwerpunkt Web/Internet.
- Problembewusstsein schaffen für die – auch bei vielen IT-Experten – noch immer ungewohnte Welt des Internet/Web.
- Problembewusstsein schaffen für die neue Dimension der Vernetztheit und Erreichbarkeit von Systemen, Daten und Informationen.
- Problembewusstsein schaffen für die Belange der IT-Forensiker.

Vorstellung aktueller und „historischer“ Vorfälle

HSH Nordbank entschuldigt sich bei ehemaligem Manager

- 20.03.2011, FAZ
- September 2009: Ein Team der Bank findet auf dem PC des New Yorker Filialleiters E-Mails, die zu **Kinderporno**-Bildern führen.
- Taggleich: Fristlose **Entlassung** des Mitarbeiters.
- September 2010: Staatsanwaltschaft erkennt und teilt mit, dass Dritte mit kriminellen Handlungen das Material untergeschoben haben.
- März 2011: HSH Nordbank kommt zum gleichen Schluss und entschuldigt sich öffentlich.
- Währenddessen: **Ablehnung bei Bewerbungen**!

http://www.faz.net/-01pzyv

Vorstellung aktueller und „historischer“ Vorfälle

Festplatten der Stadt Glücksburg landen auf Flohmarkt

- 14.12.2010, ZEIT
- Aufgrund eines Rathaus-Neubaus organisierte die Stadtverwaltung Glücksburg einen **Flohmarkt**.
- Dort wurden auch Server und Festplatten verkauft...
- Für 30 EUR erwarb ein Glücksburger 15 Festplatten und fand darauf **vertrauliche Daten** vor:
    - “Steuerbescheide, Dokumente zum umstrittenen Genehmigungsverfahren eines Spaßbades, Konzessionen für Unternehmer, Gesprächsvermerke, Protokolle und Schreiben an Bürger”.

http://www.zeit.de/digital/datenschutz/2010-12/dokumente-gluecksburg

Vorstellung aktueller und „historischer“ Vorfälle

Get in contact

- *“Welcome to the brave new world of the **13 year-old Internet terrorist**.“,*

  “[...]we can not have a stable Internet economy while 13 year-old children are free to deny arbitrary Internet services with impunity.”

  Steve Gibson, Gibson Research Corporation, 2001

(http://www.grc.com/dos/grcdos.htm)
(http://www.totse.com/en/hack/hack_attack/162022.html)

Vorstellung aktueller und „historischer“ Vorfälle

Hunderttausende gehackter Webseiten sollten Scareware verbreiten

- 01.04.2011, Heise
- Unbekannte Täter haben **hunderttausende Webseiten automatisiert angegriffen** und auf diesen eigenen schadhaften Code hinterlassen.
- Resultat: Die Besucher (also Dritte), die diese Webseiten aufriefen bekamen **Scareware** angezeigt: Einen vermeintlichen Virenscanner, der eine Infektion des eigenen PC meldete.
- Angegriffen wurden Webseiten mit **Content-Management-Systemen** eines speziellen Typs.

http://www.heise.de/newsticker/meldung/Hunderttausende-gehackter-Webseiten-sollten-Scareware-verbreiten-1219993.html

Vorstellung aktueller und „historischer“ Vorfälle

HBGary Federal vs. Anonymous

- **Anonymous**:
  - Ein **weltweit tätiges Kollektiv**
  - Tätig im Internet, aber auch außerhalb
  - “We are Anonymous.
    We are Legion.
    We do not forgive.
    We do not forget.
    Expect us!”
    – Message to Scientology-Video
- **HBGary Federal**:
  - IT-Security Unternehmen aus USA

Vorstellung aktueller und „historischer“ Vorfälle

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

Vorstellung aktueller und „historischer“ Vorfälle

HBGary Federal vs. Anonymous

Der Gegenschlag:

1. Aus dem selbst entwickelten CMS konnten per **SQL-Injection** die Passwort-Hashes des 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

Vorstellung aktueller und „historischer“ Vorfälle

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 eine **Social Engineering-Attacke** 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

Vorstellung aktueller und „historischer“ Vorfälle

HBGary Federal vs. Anonymous

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.t[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_[redacted]	l9s8d78
5514	d16b6d126b09ac17a4c37a5e503480a1		kodmaker[redacted]	cryptman
5817	cbdb7e2b1ed566ceb796af2df07205a3		plsharma-[redacted]	bond007
5838	b2f3f9771f1e9e72fc244d49adfb0142		coolsumer[redacted]	801225

Vorstellung aktueller und „historischer“ Vorfälle

HBGary Federal vs. Anonymous

- Aktuell:
  - Anwälte von HBGary Federal haben ihren ehemaligen CEO Aaron Barr unter Androhung juristischer Maßnahmen überzeugt, seine Teilnahme an der kommenden DEFCON abzusagen.
  - Quelle: Slashdot, 28.07.2011

Vorstellung aktueller und „historischer“ Vorfälle

Hacker spannt junge Mädchen per Webcam

- 16.07.2010, ZEIT
- Ein Täter aus dem Rheinland hat die **PC-Systeme von 150 Mädchen gehackt** und deren **Webcams** automatisiert abgegriffen.
- Zum Zeitpunkt der polizeilichen Durchsuchungsmaßnahme liefen parallel mehrere „Überwachungsvideos“...
- Der Täter hatte den ICQ-Account eines Schülers gehackt und kontaktierte damit seine Opfer mit der Aufforderung eine Webseite mit Bild zu öffnen.
- Diese Webseite nutzte Schwachstellen im Browser aus und verankterte einen **Trojaner** in den Opfer-PC.

http://www.stern.de/digital/online/150-faelle-hacker-spannt-junge-maedchen-per-webcam-1584091.html

Vorstellung aktueller und „historischer“ Vorfälle

Trojanisierte Android-App verrät Raubkopierer

- 02.04.2011, HotHardware
- Eine manipulierte Version der Original-App “Walk and Text” (2,10 USD) mit einer gefährlichen Funktion.
- Folgende Nachricht wird an ALLE Einträge im Adressbuch per SMS versendet:

"Hey, just downlaoded [sic] a pirated app off the internet, Walk and Text for Android. Im stupid and cheap, it costed [sic] only 1 buck. Don't steal like I did!"

http://hothardware.com/News/Shame-on-You-Pirated-Android-App-Really-Shameware/

Vorstellung aktueller und „historischer“ Vorfälle

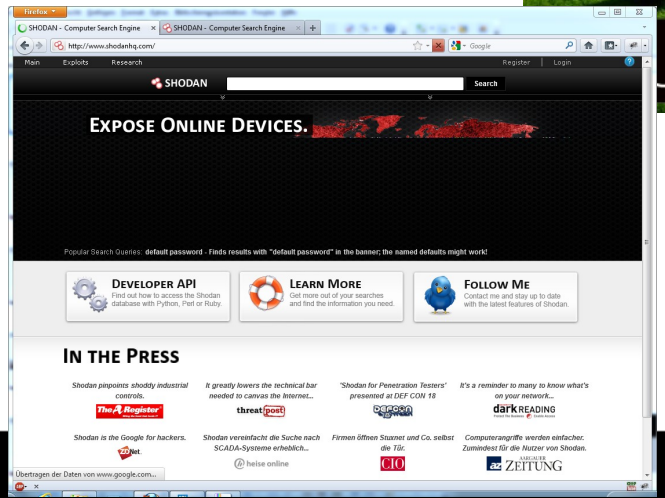
Googles Herzstück attackiert

- 19.04.2010, New York Times
- Ende 2009 gelang es Tätern mit möglicherweise chinesischem Background in das zentrale Authentifizierungssystem **Gaia** von Google einzudringen.
- Die chinesische Regierung bestreitet eine Verwicklung.
- Gaia wird für die **Single-Sign-On-Anmeldung bei Google-Anwendungen** für Millionen von Anwendern verwendet (z.B. Google Mail).
- Angriff begann mit einer Instant Message an einen Google-Mitarbeiter in China, welcher den darin enthaltenen Website-Link anklickte und darüber seinen PC infizierte.
- Durch den infizierten PC konnten die Täter auf andere Entwickler-PC und darüber auf ein **Software-Repository** zugreifen.

http://www.nytimes.com/2010/04/20/technology/20google.html

Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

- Google und SHODAN führen zu:
- Vertrauliche Daten eines CEO
- Einkäufe in einem Online-Shop
- Telefon-Flirts einer Dating-Plattform
- Drucker und Videokonferenz-System eines Anbieters für Büro- und Konferenzräume
- CISCO-Router und VoIP-Anlage eines Industrieunternehmens



Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

Vertrauliche Daten eines CEO

- Bekannter CEO mehrerer großer US-amerikanischer IT-Firmen
- Betreibt private Homepage
- Stellte mehrere GB privater Backup-Daten (inkl. Komplett-Backups seiner Thinkpads) in seinen DocumentRoot, um sie dort zu „parken“
- Enthaltene Daten: **ALLES** (Familienfotos/Kinderfotos, Finanzdaten, Verträge, Geschäftsdaten, E-Mails, Browser-History, geheime Design-Dokumente, Kalkulationen, …)
- Google-Suche: Index of /backup

Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

Einkäufe in einem Online-Shop

- US-amerikanischer Online-Shop
- Etliche umfangreiche Datensicherungen seines Quicken-Payroll-Zahlungssystems im DocumentRoot der Webseite abgelegt.
- Zwar sind diese Daten durch ein Standard-Passwort gesichert, lassen sich jedoch problemlos entpacken und als Sybase-Datenbank auswerten.
- Google-Suche: „Index of /backup“ „filetype:qpb“

Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

Telefon-Flirts einer Dating-Plattform

- Seit 5 Jahren vertrauliche Daten im Document-Root einer deutschen Partnervermittlung/Flirt-Plattform frei abrufbar.
- Es handelt sich dabei um Voice-Nachrichten von Flirtsuchenden.
- Diese Nachrichten sind eigentlich nicht mehr aktiv... (Datenschutz)
- Damalige Google-Suche:
    - -inurl:(htm|html|php) intitle:”index of” +”last modified” +”parent directory” +description +size +mp3 +voicefile
- Lieferte Tausende Sprachnachrichten im DocumentRoot.

Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

Drucker und Videokonferenz-System eines Anbieters für Büro- und konferenzräume

- SHODAN-Suche: Ricoh „200 OK“ country:DE
- SHODAN-Suche: Polycom „200 OK“ NameDesUnternehmens
- Ergebnisse:
  - Über das Internet erreichbare Drucker, ohne gesetztes Admin-Passwort, Vollzugriff, Möglichkeit eigene Firmware hochzuladen, Möglichkeit nach anderen Druckern im internen Netz zu suchen. Anzeige von Informationen über gesendete/empfangene Faxe und gedruckte Dokumente, Einrichtung einer Faxweiterleitung.
  - Über das Internet erreichbare Polycom-Konferenzanlage, ungesichert, Möglichkeit teure Rufnummern anzuwählen, Kommunikation belauschen, ...

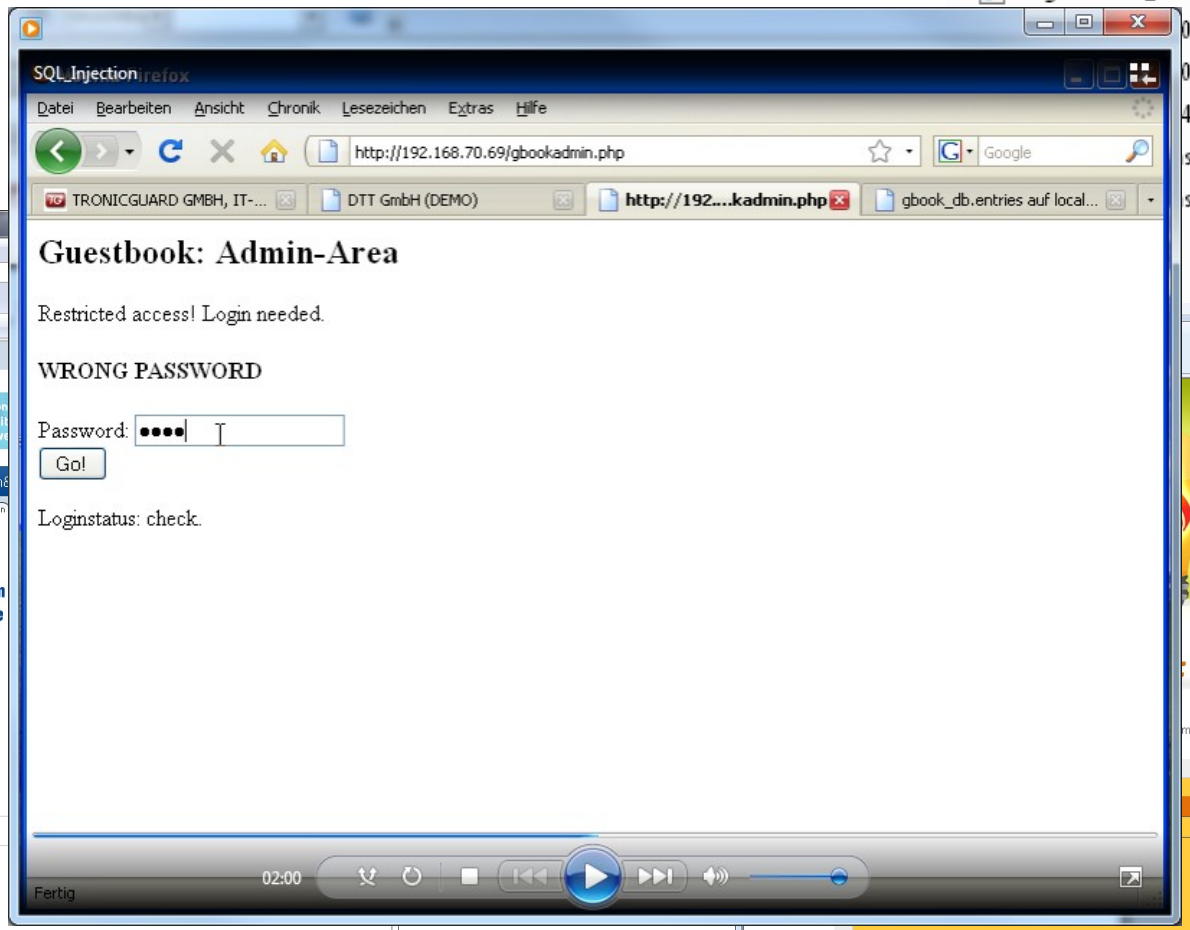
Mit Suchmaschinen-Hacks gravierende Informationslecks aufdecken

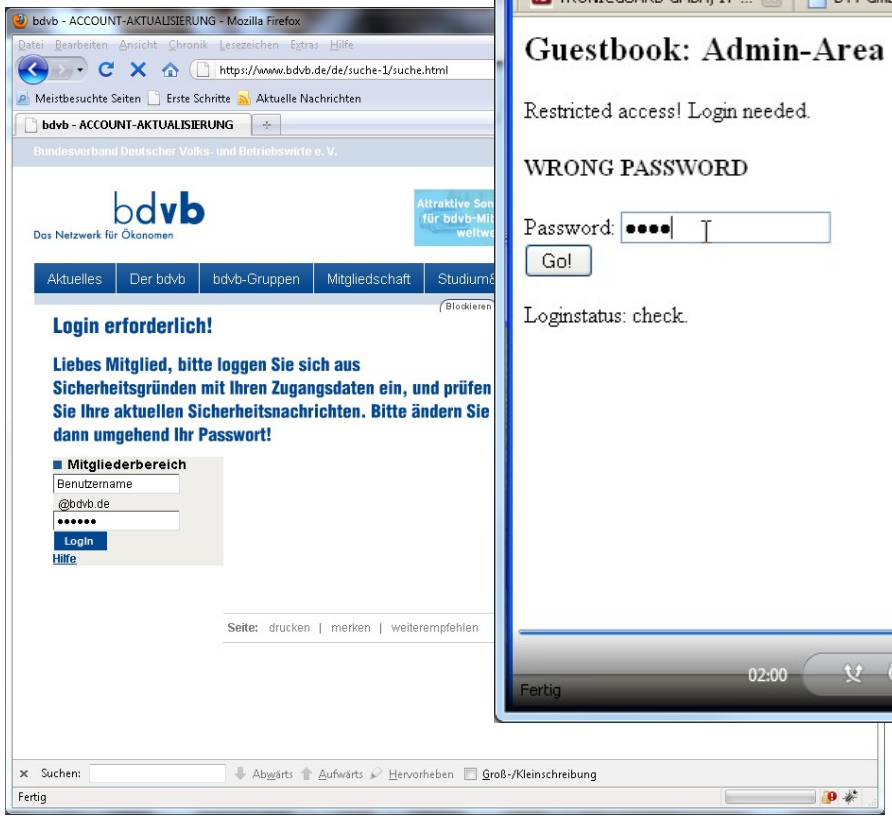
CISCO-Router und VoIP-Anlage eines Industrieunternehmens

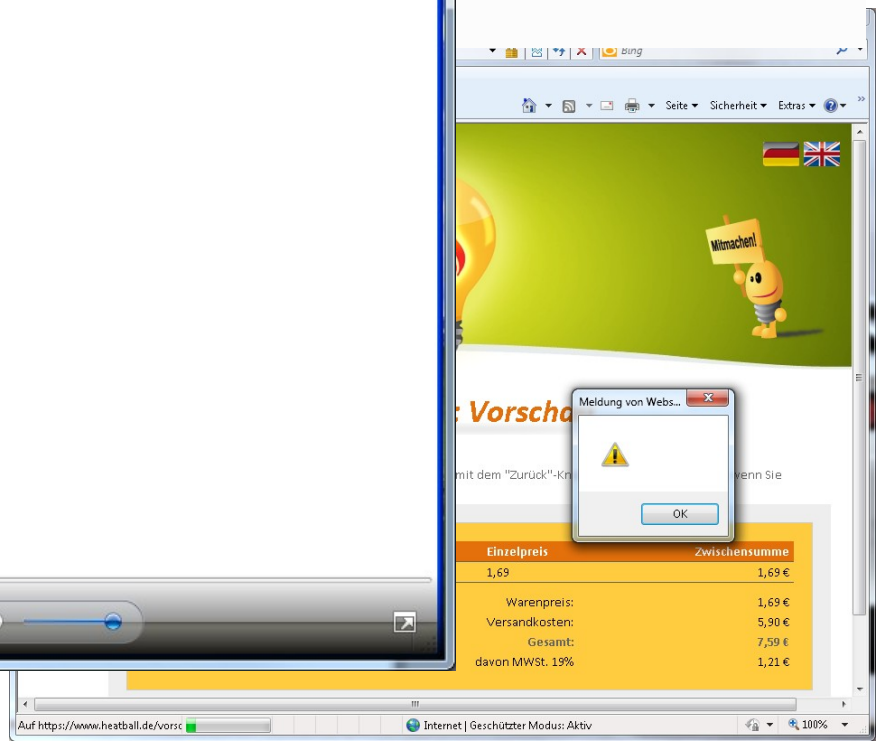
- SHODAN-Suche: cisco last-modified „200 OK“ country:DE
- SHODAN-Suche: snom embedded „200 OK“ country:DE
- Ergebnisse:
  - Ein Provider erlaubte die Exploration eines Switches.
  - Ein CISCO-Router eines deutschen Industrieunternehmens war ungeschützt (privilege level 15). Routin-Änderung war möglich!
  - Ein gefundenes Snom-System war ungeschützt, Zugriff auf: Adressbuch, Kurzwahlziele und Logfiles und sogar PCAP-Traces von laufenden Gesprächen bzw. dem Netzwerkverkehr im LAN des Telefons.

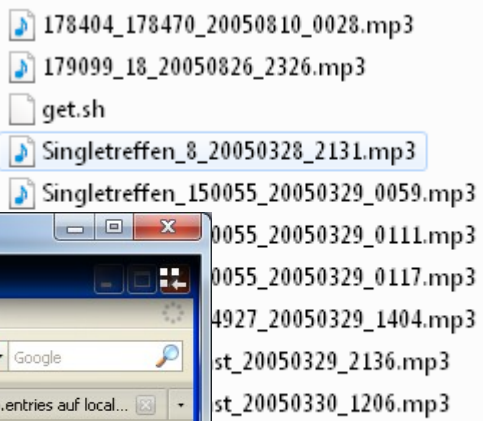
SQL-Injection und andere Fälle

- → VIDEO









Fazit 1

Herausforderung durch Web und Cloud

- Sicherheitsvorfälle nehmen rasant zu und werden **immer gefährlicher**.
- Durch massive Nachrichtenverbreitung und gesteigertes Interesse kommt es zu immer **größeren Reputationsschäden** für betroffene Unternehmen.
- „Klassische“ Fälle in der IT-Forensik treten in den Hintergrund und gestalten sich zunehmend als Routinefälle.
- Die Bedeutung von Internet und insbesondere **Web** nimmt noch immer rasant zu. Dementsprechend ändern sich die Aufgaben und Probleme für die IT-Forensik.
- Besonders **Cloud**-Techniken stellen alle Beteiligten vor große Hürden.
- Durch interdisziplinäre Qualifikation und Erfahrung können IT-Forensiker diesen Herausforderungen aber gut begegnen.

Fazit 2

Diskussion und Fragen

- :-)