

# Kompetenz zu mehr IT-Sicherheit - Konzepte zur Verbesserung der Ausbildung von IT-Fachkräften

## Den Nerv der Zeit getroffen - IT-Security Awareness in Theorie und Praxis für Kieler Masterstudierende

Martin Dombrowski und Prof. Dr. Doris Weißels

Vortrag am 25.09.2013 , Internet Security Days in Brühl



## Agenda

1. Motivation und Zielsetzung
2. Modulkonzeption
3. Inhalte und fachliche Zielsetzung in Bezug auf den Kompetenzerwerb
4. Erfahrungsbericht aus der Lehre
5. Feedback Studierende
6. Zusammenfassung und Ausblick - Der Nutzen für das wissenschaftliche und wirtschaftliche Umfeld: „Digitale Wirtschaft Schleswig-Holstein“ und Hochschulen in Kiel
7. Résumé und Diskussion



## Referenten

### Martin Dombrowski

Security Engineer Central EMEA,  
Imperva Ltd.



### Prof. Dr. Doris Weßels

- Professur für Wirtschaftsinformatik an der Fachhochschule Kiel - <http://www.fh-kiel.de/index.php?id=5340>
- Vorstandsmitglied der Digitalen Wirtschaft Schleswig-Holstein mit dem Schwerpunkt Transfer Wirtschaft und Wissenschaft - <http://www.diwish.de/vorstand.html>
- Kontakt: [doris.wessels@fh-kiel.de](mailto:doris.wessels@fh-kiel.de)



## Motivation: Cyber-Attacken auf dem Vormarsch

- Immer häufiger werden Unternehmen und Organisationen durch sogenannte Cyber-Attacken bedroht.
- Daher wird das Thema Cybersicherheit von Experten als Standortfaktor der Zukunft bewertet.
- Wie können wir als zukunftsorientierte Hochschule die Studierenden aktiv auf dieses Thema vorbereiten?
- Die Idee: Schaffung eines neues Modulangebots im Sommersemester 2013:  
**„IT-Security Awareness in Theorie und Praxis –  
Einstieg in die Cyber-Forensik“**

*an der Fachhochschule Kiel in Kooperation mit dem Institut für  
Wirtschaftsinformatik an der CAU*



- mit einem Experten als Lehrenden: Martin Dombrowski

## Modulkonzeption

<b>Dauer des Moduls</b>	3 Samstage: 04. Mai, 11. Mai und 18. Mai von 9-17 Uhr
<b>Art des Moduls (Pflicht, Wahl, etc.)</b>	Wahlpflichtmodul (vorrangig für den Masterstudiengang Wirtschaftsinformatik)
<b>Zugangsvoraussetzungen</b>	Netzwerkgrundlagen und IT-Affinität bzw. Interesse an IT-Sicherheit und Cyber-Forensik
<b>Verwendbarkeit des Moduls für andere Studiengänge</b>	<ul style="list-style-type: none"> <li>• Teilnahmemöglichkeit auch für Studierende anderer Fachbereiche</li> <li>• Hinweis: Bachelorstudierende der Wirtschaftsinformatik sind ebenfalls willkommen.</li> <li>• ggf. auch hochschulübergreifend genutztes neues Modulangebot</li> </ul>
<b>Zahl der zugeteilten ECTS- Credits</b>	5
<b>Gesamt-Workload des Moduls</b>	Präsenzzeit: ca. 24 Stunden (3x8=24 Stunden) Vor- und Nachbereitung: ca. 63 Stunden Klausurvorbereitung: ca. 63 Stunden
<b>Art der Prüfung/ Voraussetzung für die Vergabe von Leistungspunkten</b>	<ol style="list-style-type: none"> <li>1. Teilnahme und engagierte Mitarbeit an den Präsenzblöcken</li> <li>2. erfolgreiches Bestehen der schriftlichen Prüfung</li> </ol>
<b>Qualifikationsziele des Moduls</b>	<ol style="list-style-type: none"> <li>1. IT Security Sensibilisierung</li> <li>2. Wissen über IT Security Lösungen und Herausforderungen</li> <li>3. Verständnis über aktuelle Angriffsvektoren</li> </ol>
<b>Lehr- und Lernmethoden</b>	<ol style="list-style-type: none"> <li>1. Vortrag</li> <li>2. Interaktion mit Teilnehmern</li> <li>3. Live-Vorfürungen</li> </ol>

## Detailsichtweise

### TAG 1

- Die Evolution der Wirtschaftsspionage und Internetkriminalität und die daraus resultierenden Herausforderungen
- Hacktivismus und der Insider Threat
- Historische Entwicklung der IT Security
- Übersicht über IT Security Lösungen und deren Funktionsweise
- Einblicke in neueste IT Security Technologien und Ansätze

### TAG 2

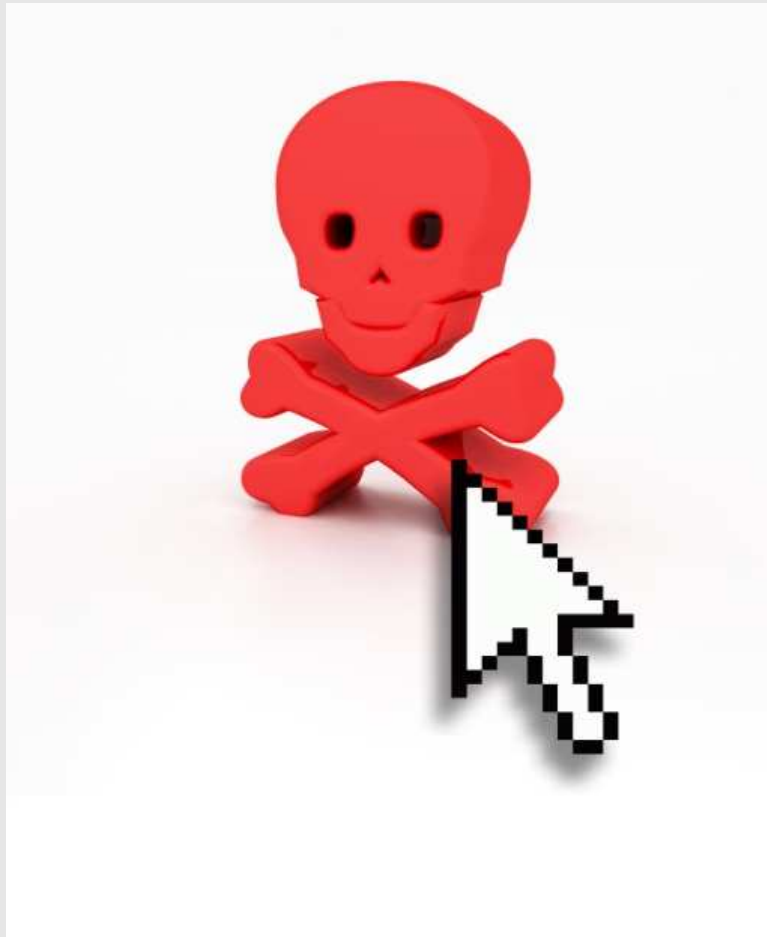
- Kenne Deinen Feind. Einblicke in die Phasen des Hackings
- Vorbereitung
- Informationsbeschaffung
- Risikobewertung
- Aktive Eindringversuche
- Aufbau des Testinglabs
- Hackingslabs
- Web Ressourcen und Google Hacking
- Port Scanning
- Arp Spoofing
- Buffer Overflow exploitation
- Working with exploits
- transferring files
- exploit frameworks
- Client side attacks
- Tunneling & Port forwarding
- Password Attacks
- Physical Access Attack
- Web Application Attack Vectors
- Alternate Data Stream
- Rootkits

### TAG 3

- Weiterführung praktischer Übungen
- Klausur



## Beispielhafter Einblick in das Thema



# Sensibilisierung

# Ausgereifte Strukturen im Handel mit gestohlenen Daten

WE-SELL.CC

- ✓ Creditcards
- ✓ Packstation

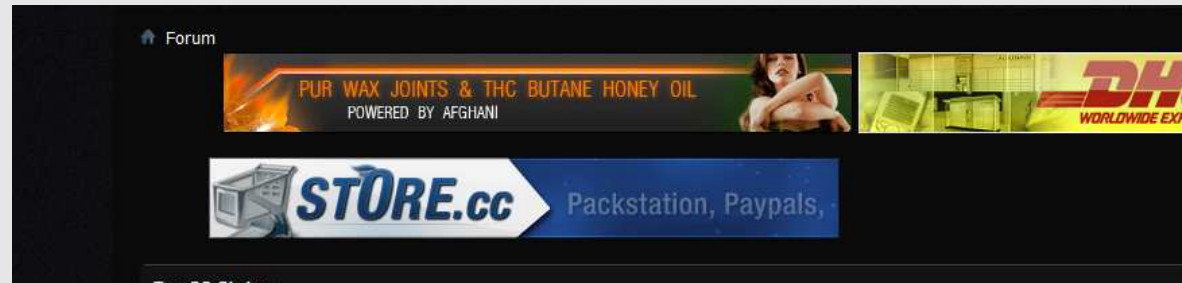
[Artikelname]	[Preis]
AG CC (German)	14.99
Doktor/Firma - German CC	9.99
Firmeninhaber CC (German)	14.99
German CC [Mastercard]	7.99
German CC [Visa]	7.99
Unchecked Ger CC [90 % Valid]	5.99

AGB

This script is property of Tamashi-store



# Internetforen



CARDERS.cc v3

Forum Was ist neu?

Benutzerkontrollzentrum • Private Nachrichten • Posteingang • AWI: PP

**WICHTIG!**  
**Bitte beachtet die neuen Regeln:**  
- keine Posts im Hauptplatz erlaubt (siehe hier)  
- keine Posts im Vorstellungsbereich erlaubt (siehe hier)  
- neue Forumregeln (siehe hier)  
**Verstöße gegen diese Regeln werden mit Timeouts bestraft!**

Private Nachrichten

- Posteingang
- Postausgang
- Neue Nachricht
- Nachrichtenverfolgung
- Ordner bearbeiten

Abonnements

- Abonnements anzeigen
- Ordner bearbeiten

Einstellungen

- Mein Profil
- Profil bearbeiten

Dr. Carder  
Benutzer

AWI: PP  
mit CC: hier: 401: 632763

Wollen Sie...  
Direkt antworten

10 € PSC [S] 10 € Ukash  
111.6

Post	Reaktionen	Benutzer
10 € PSC [S] 10 € Ukash	0 0	Insta
10 € PSC [S] 10 € Ukash	69 14	Insta
EXCHANGE INSTANT	129 8	Cr
trollt die Post?	109 12	JimPa
Suche Exchanger	30 5	KR
-holland_Weed [S]LR,PSC	374 11	anu
Seeds White...	91 5	st
EE]MOFOS[FRISCH FAKED!!!]	486 65	cra
2 Real Plastik...	176 10	bank_of_g
dieren ohne Fachabitur?	151 9	hazehazel
1A TROJANER V3[NEU - 2012]	186 9	Lu
EE] Uploadet.to	378 47	klei
deutscher CC nach Österreich...	0 0	lalal
Trusted Seller für fertiges...	20 2	wind
1 Versand nach DE - Droppen...	34 2	G
EE] Cebit 2012 Tickets	211 15	ne
Anabolika Tabletten [B]...	0 3	aLph4
1 Gram "HASCÖL" HQ [KEINE...	0 1	G
blem beim Topic eröffnen	39 3	Lu

## Die Presse.com › Tech › Internet › Sicherheit

Politik Wirtschaft Panorama Kultur Tech Sport Leben Bildung Wissenschaft Gesundheit Recht

# Bericht: 15-jähriger Hacker knackte PCs von 259 Firmen

13.04.2012 | 18:15 | (DiePresse.com)

**Ein Schüler aus Niederösterreich soll von seinem Kinderzimmer aus Codes und Passwörter von Unternehmen geknackt und ins Internet gestellt haben. Öfters hinterließ er mysteriöse "Grüße". Der Junge wurde angezeigt.**



 Bild vergrößern

 Drucken

 Senden

Für einen 15-Jährigen aus Niederösterreich war es möglicherweise ein Spiel. Für Angehörige des Bundeskriminalamts waren es - so die Tageszeitung "**Kurier**" - "beinhart geführte Hackerangriffe auf Firmen in Österreich und Europa". Im Zeitraum von Jänner bis März dieses Jahres hatte der Jugendliche von seinem Kinderzimmer aus die Codes und Passwörter von 259 Unternehmen geknackt und diese ins Internet gestellt, heißt es in dem Bericht.

06.10.2012 16:36

 « Vorige | Nächste »

## Vorratsdatenspeicherung in der Polizeipraxis

 vorlesen / MP3-Download

Dank der in Frankreich praktizierten Vorratsdatenspeicherung von 12 Monaten Dauer konnte der Anschlussinhaber in Nantes ermittelt werden und dank eines weiteren Fehlers (Anmeldung auf Facebook mit der IP-Adresse) wurde der Täter gefasst, ein 16-jähriger Franzose. Ein Skript-Kiddie, das im **Alter von 14 Jahren** mit dem **"Hacken" begonnen** hatte und vom **Anschluss seiner Großeltern** aus die digitale Welt erkundete. Manske stellte klar: "Wir hätten den Tatnachweis aufgrund der ausgesetzten Vorratsdatenspeicherung nicht in Deutschland führen können". Zur politischen Diskussion ergänzte er: "QuickFreeze ist ein völlig ungeeignetes Mittel. Ohne VDS hätte wir warten müssen, dass er noch einen Fehler macht".

Teamleiter Cybercrime beim BKA, von ihm stammen die Zahlen zur Vorratsdatenspeicherung, die BKA-Chef Ziercke bei seiner [Argumentation für die VDS](#) anführt. Manske berichtete ausführlich vom Fall ZyklonB, den das BKA erfolgreich abschließen konnte, weil in Frankreich die Verbindungsdaten auf Vorrat gespeichert werden.

# Havij

**Target:** `http://localhost/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1`

**Keyword:** Auto Detect     **Syntax:** Auto Detect

**Data Base:** Auto Detect    **Method:** GET    **Type:** Auto Detect

**Tools:** About, Info, Tables, Read Files, Cmd Shell, Query, Find Admin, MD5, Settings

**Actions:** Stop, Get DBs, Get Tables, Get Columns, Get Data, Save Tables, Save Data

**Database Tree:** dvwa
 

- users
  - avatar
  - password
  - user
  - last\_name
  - first\_name
  - user\_id
- guestbook

user	password
admin	5f4dcc3b5aa765d61d8327deb...
<b>gordonb</b>	<b>e00a18c428cb38d5f2608536...</b>
1337	75ae2c3966d7e0d4f...
pablo	af5bbe40cade3de5c...
smithy	5a5765d61d8327deb...

Use Group\_Concat (MySQL Only)     All in one request

Status: I'm IDLE    Clear Log

```
Count(column_name) of information_schema.columns Where table_schema=0x64767761 AND table_na
Columns found: user_id,first_name,last_name,user,password,avatar
GET [redacted].php?id=106147073' and ascii(substring((SELECT distinct table_name FROM information_sche
ma.tables Where table_schema=0x202020 limit 0,1),2,1))=56 and 'x'='x' HTTP/1.1
Host: [redacted]
Accept: */*
User-Agent: Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 5.1; SV1; .NET CLR 2.0.50727) Havij
Connection: Close
```

# Wie Unternehmen gezielt angegriffen werden...

The screenshot shows the LinkedIn 'Advanced People Search' interface. A red rectangular box highlights the 'Title' and 'Company' search fields. The 'Title' field contains 'DBA' and has a 'Current' dropdown menu. The 'Company' field contains 'Bank of America' and also has a 'Current' dropdown menu. Other search criteria include 'Keywords', 'First Name', 'Last Name', 'Location' (set to 'United Kingdom'), 'Postal Code', and 'Within' (set to '50 mi (80 km)'). A 'Search' button is located below the search criteria. On the right side, there is a 'Premium Search' advertisement with a list of tools and an 'Upgrade' button.

LinkedIn Account Type: Basic | Upgrade

Home Profile Contacts Groups Jobs Inbox Companies News More People Search...

Find People **Advanced People Search** Reference Search Saved Searches

Keywords:

First Name:

Last Name:

Location: Located in or near:

Country: United Kingdom

Postal Code:  Lookup

Within: 50 mi (80 km)

**Title:** DBA  Current

**Company:** Bank of America  Current

School:

Industries:  All Industries

Seniority Level:  All Seniority Levels

**Premium Search**  
Find the right people in half the time

**Premium Search Tools:**

- Premium filters
- Automatic search alerts
- Full profile access

or [Learn more](#)

## ...Dank sozialer Netzwerke effektiver und einfacher

The screenshot shows a LinkedIn search results page with 24 results. The search filters are set to 'People' and 'Search...'. The results are sorted by 'Relevance' and shown in 'Expanded' view. The first four results are highlighted with red boxes:

- SQL DBA at BP**: London, United Kingdom · Information Technology and Services · 117 connections. Current: SQL DBA at Bank of America Merrill Lynch. Past: SQL Sybase Team Leader at DataCom. Groups: SQL Server Elite · City Infrastructure.
- Sybase DBA at Bank of America**: United Kingdom · Banking · 74 connections. Current: Sybase DBA at Bank of America, ybase. Past: Sybase DBA at UBS, Sybase DBA at.
- LinkedIn Member**: Database Administrator at Merrill Lynch · Reading, United Kingdom · Banking · 31 connections. Current: DBA at Bank of America, Database. Past: DBA at Centrica.
- Oracle DBA at Bank of America**: St Albans, United Kingdom · Information Technology and Services · 450 connections · 2 recommendations. Current: Oracle DBA at Bank of America. Past: Oracle DBA at Credit Suisse Bank. Groups: Global Oracle Contractors Network.

Each result includes a 'Send InMail' button. The right sidebar features 'Premium Search' options and an 'Upgrade' button.

# Smart Bombing am Beispiel Facebook

### Review Ad Help

Ad Name: **I Want to Work for Google**

Audience: You are targeting people age 18 and older in the United States who work at Google.

Campaign: My Ads (New Campaign)

Bid Type: CPC

**Get a Job** Daily Budget **\$10.00** Since 08/06/2008

Name	Bid (\$)	Type	Imp.	Clicks	CTR (%)	Avg. CPC (\$)	Avg. CPM (\$)	Spent (\$)
Hiring?	0.50	CPC	26	0	0.00	0.00	0.00	0.00
I want to work for Oxford	0.40	CPC	622	20	3.22	0.26	8.30	5.16
<b>Totals</b>			648	20	3.09	0.26	7.96	5.16

Choose a graph: **Clicks**

State/Province/Region:

Zip/Postal Code:

This information will be saved to your account.

**Coupon**

Coupon Code: **5V6-1JKV-TNH9-2MRH**

## Feedback Studierende (1)

### ■ Atmosphäre:

Mein persönlicher Gesamteindruck ist "sehr gut". Der Stimmung der anderen Kommilitonen nach waren auch sie begeistert. Man hat viel gelernt und wurde auch sensibilisiert.

### ■ Abgrenzung zum vorhandenen Modul „IT-Sicherheit“:

Dort geht es vorwiegend um die *Absicherung von IT-Systemen*, während Herr Dombrowski die *Schwachstellen von IT-Systemen* aufgezeigt hat.

Einen Nachteil darf man meiner Meinung nach allerdings nicht außer Acht lassen: Das Wissen, welches man bei Herrn Dombrowski gelernt hat, kann auch missbraucht werden.

### ■ Kooperation der Hochschulen:

Kontakte und Erweiterung des Netzwerkes über die Hochschulgrenzen hinweg finde ich sehr positiv.





## Feedback Studierende (2)

### ■ Rahmenbedingungen:

Die Veranstaltung hat einen sehr guten Praxisbezug, Herr Dombrowski hat auf mich durchgehend einen sehr kompetenten Eindruck gemacht und die Themen gut vermittelt. Vor allem die Einbeziehung der Studenten in kurzen Hacking-Übungen war sehr interessant und hat die ganze Veranstaltung sehr gut aufgelockert.



### ■ Relevanz:

Ich denke gerade als Wirtschaftsinformatiker ist es wichtig zu wissen, wie wichtig IT-Security im Betriebskontext ist. Gerade die schockierende Einfachheit eines Hackerangriffs, die Herr Dombrowski uns gezeigt hat, macht einen für dieses Thema viel sensibler. Von daher ist ein regelmäßiges Angebot auf jeden Fall eine Gewinn für den Studiengang.



### ■ Ausbau:

Die Veranstaltung könnte noch einen etwas größeren theoretischen Block bekommen, um die Grundlagen von Hackingangriffen zu erklären. Wenn man nicht sehr technisch interessiert ist, sind einem die Möglichkeiten der Angriffe wohl eher unklar.

# Relevante Technologieschwerpunkte der Digitalen Wirtschaft Schleswig-Holstein (DiWiSH)

Mit dem Ziel die IT- und Medienbranche in Schleswig-Holstein zu fördern, konzentriert sich das Clustermanagement DiWiSH u.a. auf folgende Zielsetzungen

## 1. Abbau des Fachkräftemangels

Eines der größten Probleme der IT- und Medienbranche in Schleswig-Holstein wie auch bundesweit ist der Fachkräftemangel. Eine gezielte Förderung des Nachwuchses ist daher dringend erforderlich.



## 2. Technologieschwerpunkt „Internet der Zukunft“

Das Dienstleistungsangebot des Clusters DiWiSH umfasst das Initiieren von Innovationen, die Förderung des Know-How-Transfers und die Unterstützung von Unternehmensgründungen. Dazu werden Veranstaltungen zu aktuellen Themen wie Cloud Computing, Medienkonvergenz und Social Media angeboten.

# Impuls – Der Weg zur Gründung einer Fachgruppe unter dem Dach der Digitalen Wirtschaft Schleswig-Holstein

1. Kooperation mit FH- und Universitätskollegen sowie Experten der **Wirtschaft**
2. Das Ergebnis ist positiv: Die **Sammlung aller Module** aus FH- und Uni Kiel und die Bereitschaft der Wirtschaft zur Mitwirkung spiegelt erstaunlich viel Expertise und Potenzial in SH wider. Als Kieler Hochschulen würden wir daher gerne zukünftig hochschulübergreifende Angebote stärker anbieten – im engen Dialog mit der Wirtschaft bzw. Praxis (falls Prüfungsämter etc. hier mitspielen...)
3. Um dieses bedeutende IT-Thema in SH „sichtbar“ zu machen für beide Seiten (Bedarfsträger und Anbieter) und Hochschulen und Wirtschaft stärker zu verbinden, wird die **Gründung einer neuen DiWiSH-Fachgruppe** initiiert

**Vision:** Darüber hinaus könnte die Verbindung des Angebotes der Hochschulen und der Einsatz im „Business“ den (visionären) Ausbau zu einem „Kompetenzzentrum“ (o.ä.) sinnvoll erscheinen lassen. Besonders interessant erschien in den Diskussionen die Möglichkeit des Erwerbs **eines DiWiSH-Zertifikats zum Thema „IT-Security“ (o.ä.) als Nachweis der persönlichen Expertise – ein interessantes neues Serviceangebot.**



## Zusammenfassung

- In IT-nahen Studiengängen stellt es eine besondere Herausforderung dar, zeitgemäße Themen und absehbare Qualifizierungsbedarfe „passgenau“ für alle Beteiligten in den curricularen Aufbau zu integrieren.
- An der Fachhochschule Kiel wurde im Sommersemester 2013 erstmalig das Modul "IT-Security Awareness in Theorie und Praxis – Einstieg in die Cyber-Forensik" für Masterstudierende der Kieler Hochschulen angeboten.
- Die Resonanz des Teilnehmerkreises bestätigte den Verdacht, dass hiermit eine wichtige Angebotslücke geschlossen werden konnte.
- Der Vortrag beleuchtet neben der Motivation auch den Rahmen der Durchführung und die positiven Nutzeneffekte im Know-how-Transfer und Dialog mit der Wirtschaft.

# Résumé und Diskussion

