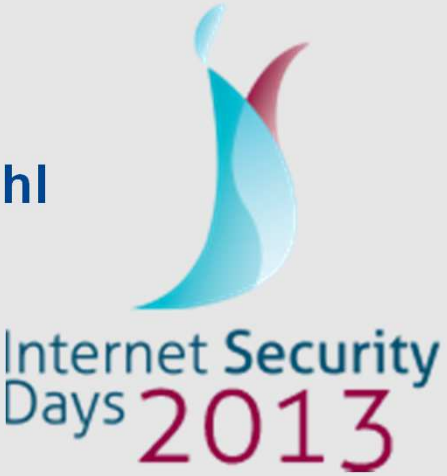
Kompetenz zu mehr IT-Sicherheit - Konzepte zur Verbesserung der Ausbildung von IT-Fachkräften

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

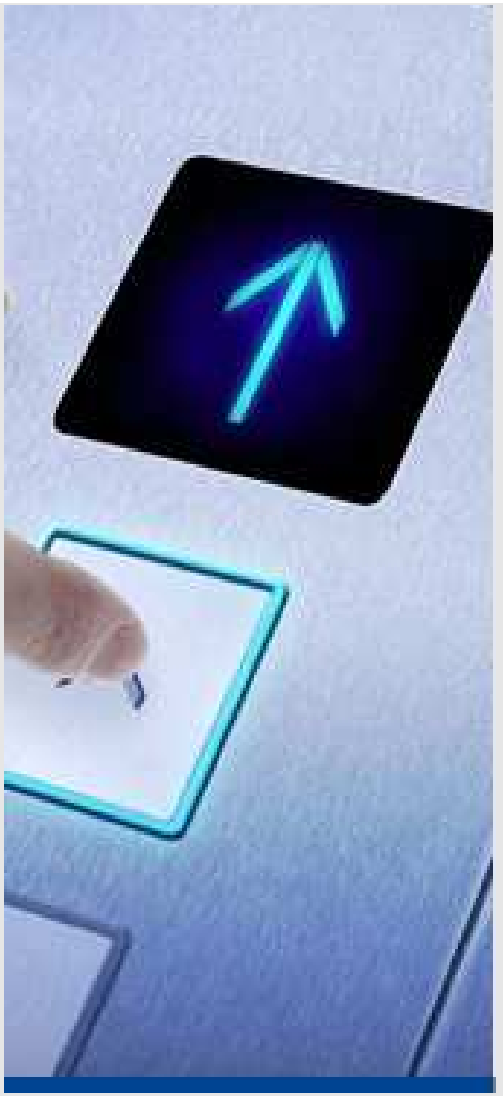
Martin Dombrowski und Prof. Dr. Doris Weßels

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

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

Dauer des Moduls	3 Samstage: 04. Mai, 11. Mai und 18. Mai von 9-17 Uhr
Art des Moduls (Pflicht, Wahl, etc.)	Wahlpflichtmodul (vorrangig für den Masterstudiengang Wirtschaftsinformatik)
Zugangsvoraussetzungen	Netzwerkgrundlagen und IT-Affinität bzw. Interesse an IT-Sicherheit und Cyber-Forensik
Verwendbarkeit des Moduls für andere Studiengänge	• Teilnahmemöglichkeit auch für Studierende anderer Fachbereiche • Hinweis: Bachelorstudierende der Wirtschaftsinformatik sind ebenfalls willkommen. • ggf. auch hochschulübergreifend genutztes neues Modulangebot
Zahl der zugeteilten ECTS-Credits	5
Gesamt-Workload des Moduls	Präsenzzeit: ca. 24 Stunden (3x8=24 Stunden) Vor- und Nachbereitung: ca. 63 Stunden Klausurvorbereitung: ca. 63 Stunden
Art der Prüfung/ Voraussetzung für die Vergabe von Leistungspunkten	1. Teilnahme und engagierte Mitarbeit an den Präsenzblöcken 2. erfolgreiches Bestehen der schriftlichen Prüfung
Qualifikationsziele des Moduls	1. IT Security Sensibilisierung 2. Wissen über IT Security Lösungen und Herausforderungen 3. Verständnis über aktuelle Angriffsvektoren
Lehr- und Lernmethoden	1. Vortrag 2. Interaktion mit Teilnehmern 3. Live-Vorführungen

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 derer Funktionsweise
- Einblicke in neueste IT Security Technoiogien und Ansätze

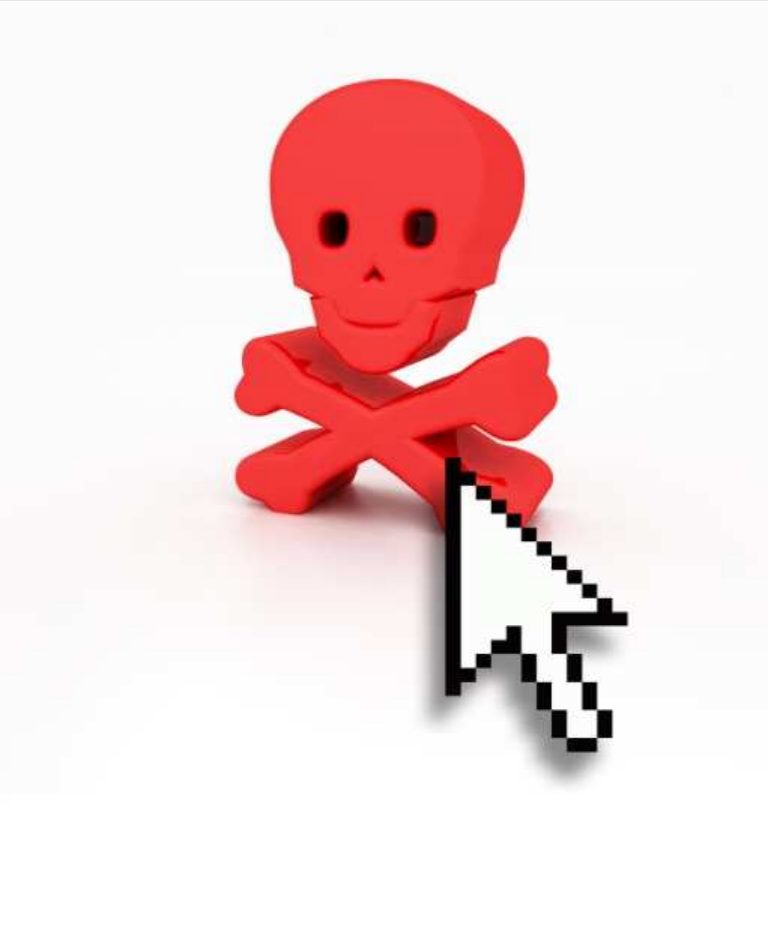
TAG 2

- 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
- transfering 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

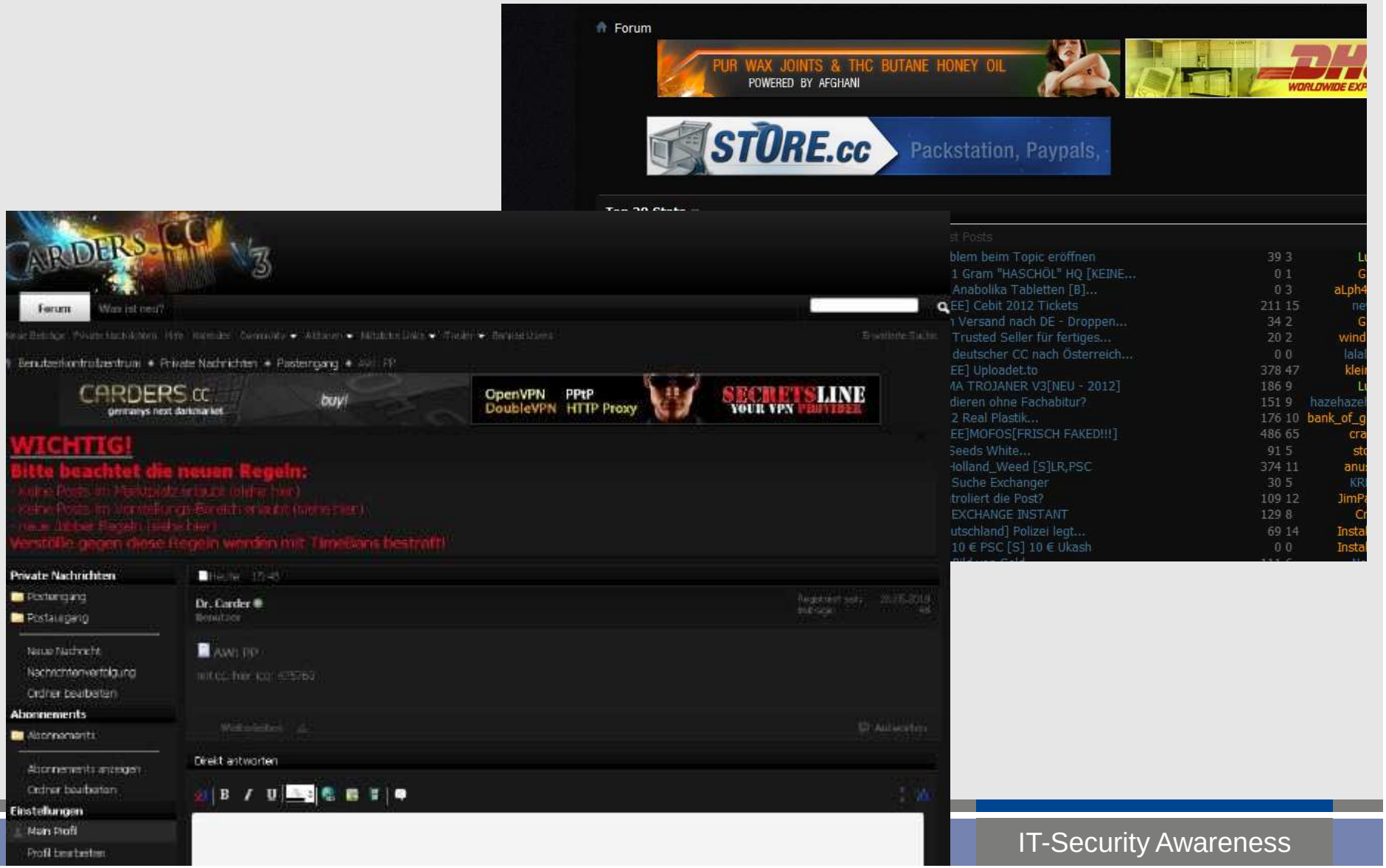
Beispielhafter Einblick in das Thema



Sensibilisierung

Ausgereifte Strukturen im Handel mit gestohlenen Daten

Internetforen



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 »

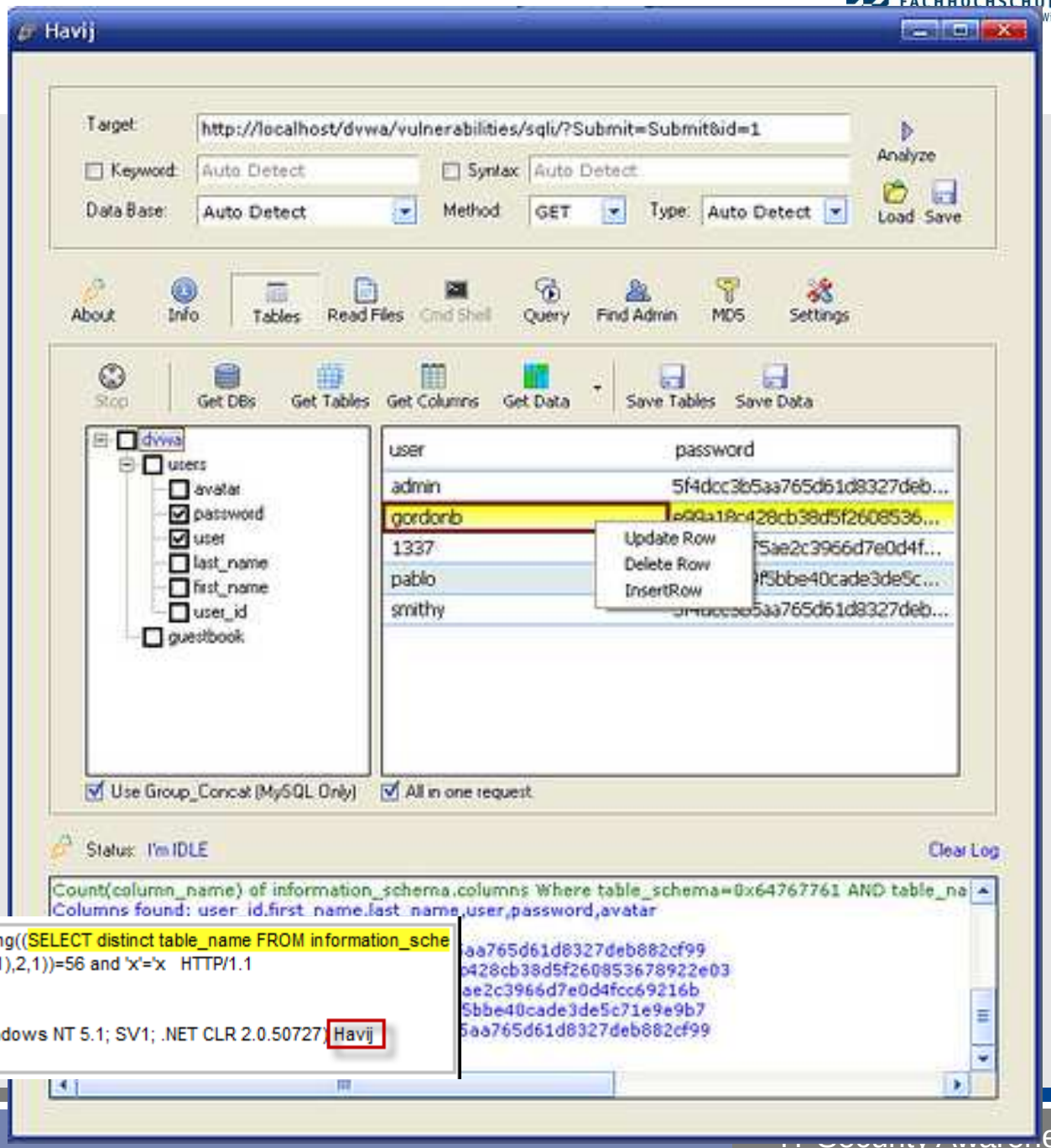
Vorratsdatenspeicherung in der Polizeipraxis

vorlesen / MP3-Download

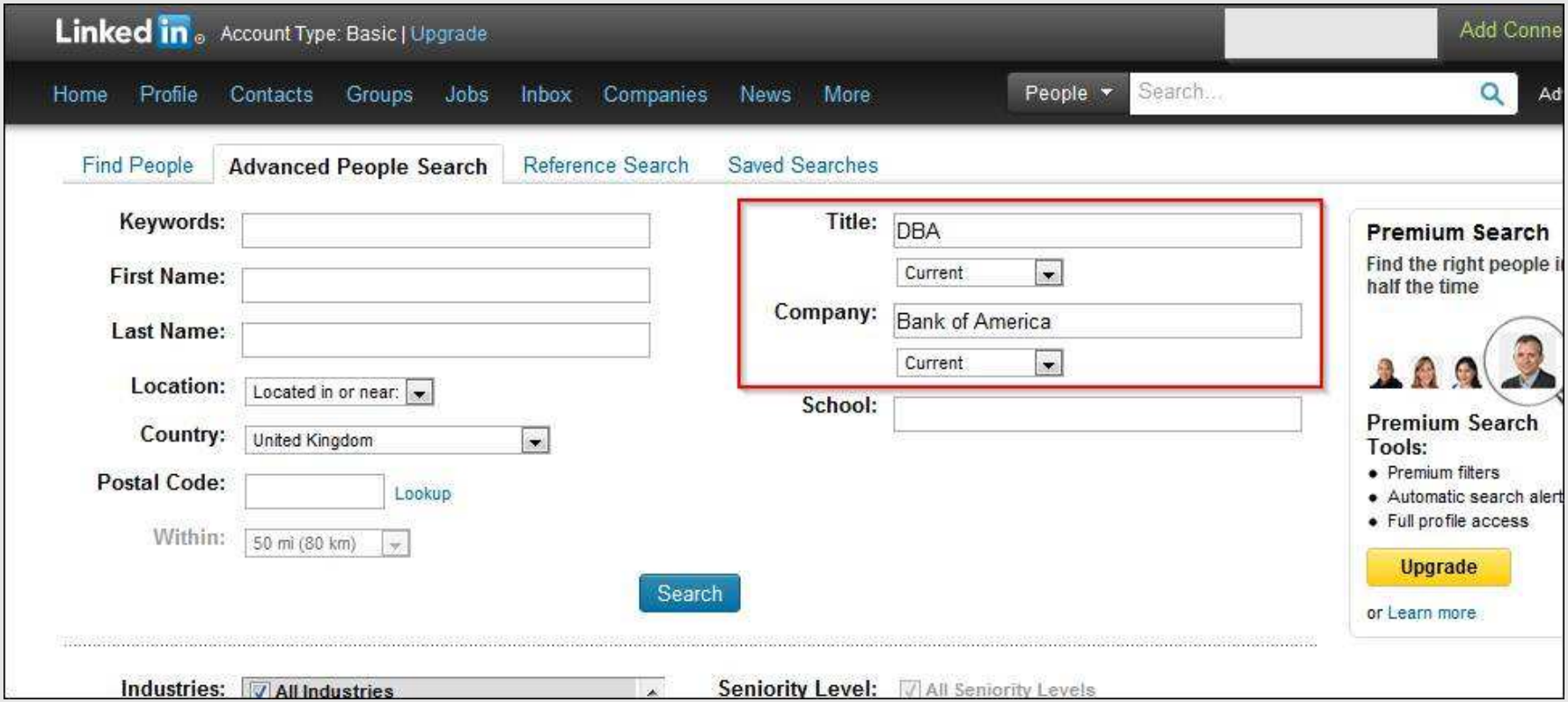
Dank der in Frankreich praktizierten Vorratsdatenspeicherung von 12 Monaten Dauer konnte der Anschlussinhaber in Nantes ermittelt werden und dank eines weiteren Fehlers (Anmeldung auf Facebook mit der IP-Adresse) wurde der Täter gefasst, ein 16-jähriger Franzose. Ein Skript-Kiddie, das im Alter von 14 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".

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.

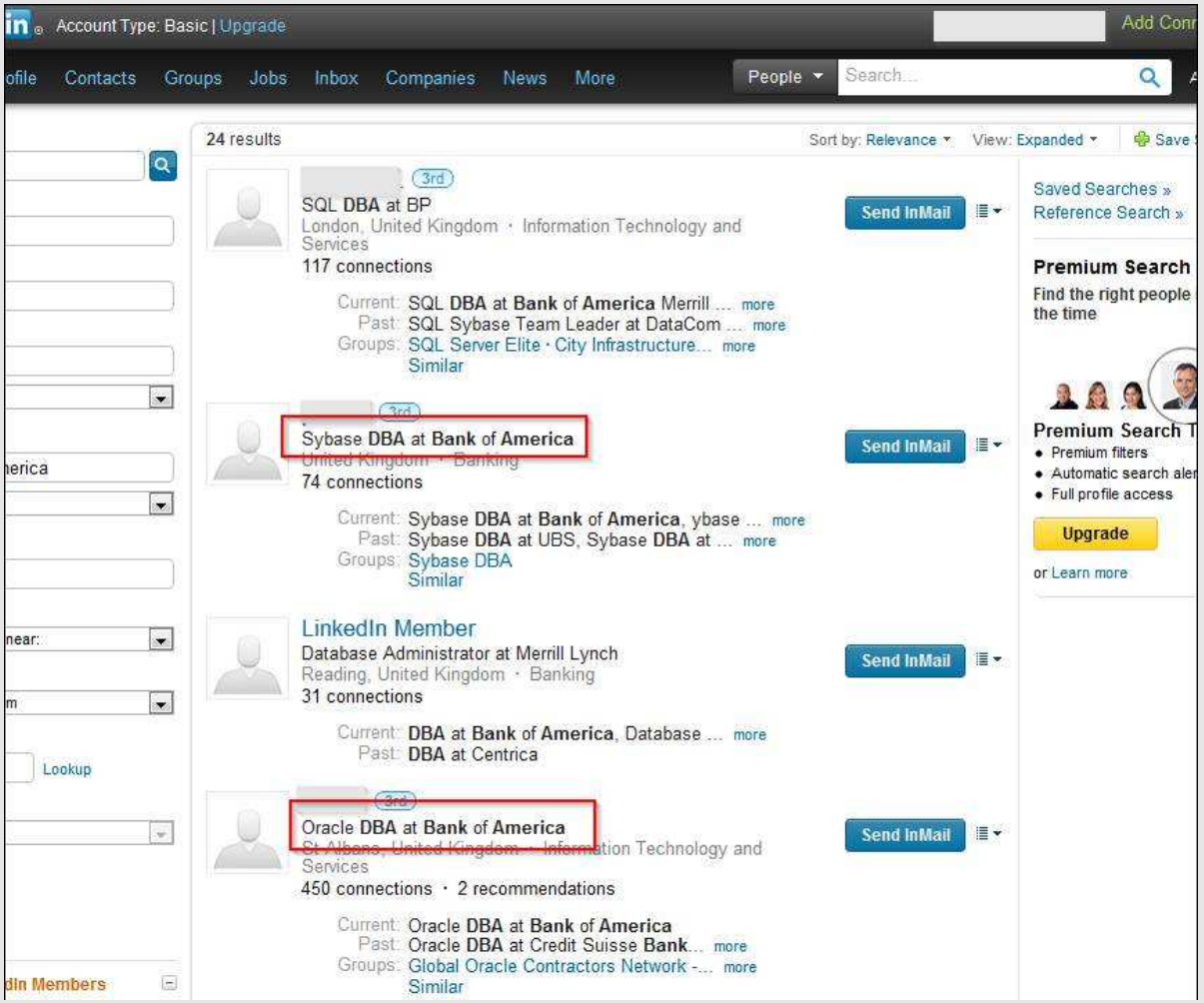
Havij


Havij
Target: http://localhost/dvwa/vulnerabilities/sqli/?Submit=Submit&id=1
Analyze
Keyword: Auto Detect
Syntax: Auto Detect
Data Base: Auto Detect
Method: GET
Type: Auto Detect
Load
Save
About
Info
Tables
Read Files
Cmd Shell
Query
Find Admin
MD5
Settings
Stop
Get DBs
Get Tables
Get Columns
Get Data
Save Tables
Save Data
dvwa
users
avatar
password
user
last_name
first_name
user_id
guestbook
user
password
admin
5f4dcc3b5aa765d61d8327deb...
gordonb
1337
pablo
smithy
Update Row
Delete Row
InsertRow
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
aa765d61d8327deb882cf99
p428cb38d5f260853678922e03
ae2c3966d7e0d4fcc69216b
5bbe40cade3de5c71e9e9b7
5aa765d61d8327deb882cf99
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

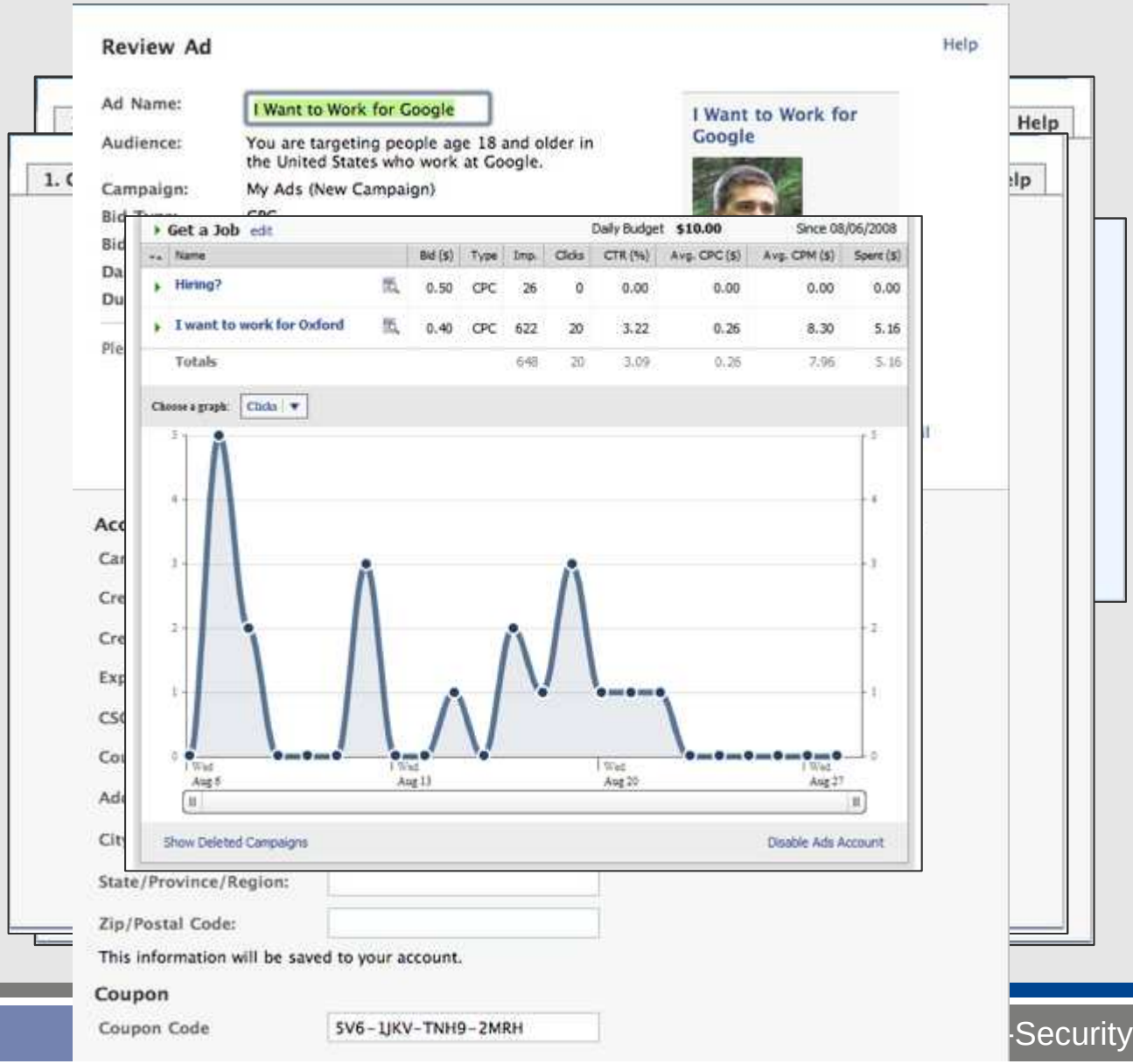
Wie Unternehmen gezielt angegriffen werden…



…Dank sozialer Netzwerke effektiver und einfacher



Smart Bombing am Beispiel Facebook



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

FACHHOCHSCHULE KIEL
Hochschule für Angewandte Wissenschaften
Internet Security Days 2013

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