

Donnerstag, 19. November 2015, 09 -10
3. DACH-Sicherheitsforum, Going, Tirol

Social Engineering via Social Media

Mechanismen, Schutzmassnahmen und Trends

Peter Heinzmann, Prof. Dr. sc. Techn.

Professor für Computernetze und Informationssicherheit, HSR Hochschule für Technik Rapperswil,
cnlab information technology research ag
Obere Bahnhofstrasse 32b, 8640 Rapperswil
www.cnlab.ch peter.heinzmann@cnlab.ch +41 55 2143330



Peter Heinzmann

cnlab AG, Obere Bahnhofstrasse 32b
Tel. +41 55 214 3330
peter.heinzmann@cnlab.ch

Dipl. El. Ing. ETH
(Diplomarbeit: Public Key Crypto Systeme)
Dr. sc. techn.
(Dissertation: Glasfasertechnik und Netzwerke)

- 1980 - 86 Eidgenössische Technische Hochschule Zürich (ETHZ)
 - Optische Kommunikationsnetze
- 1987-91 IBM Research Laboratory, Rüschlikon
 - Token-Ring Gruppe
 - High Speed Networking
- 1991 - HSR Hochschule für Technik Rapperswil
 - Professor für Computernetze und Informationssicherheit
- 1997 - Techn. Direktor cnlab AG



information technology
research

Produkte und Dienstleistungen

Publikationen

Über cnlab itr

Mitarbeiter

Kontakt

information technology research

cnlab ist eine Gruppe von drei Engineering-Firmen im IT-Bereich. Wir arbeiten in den Bereichen IT-Sicherheit, Netzwerkperformance und Software-Entwicklung. Die cnlab-Organisationen sind Aktiengesellschaften nach Schweizer Recht mit Sitz in Rapperswil-Jona. Sie sind alle im Besitz des Managements.

cnlab Speed Test
cnlab AG Tools ★★★★☆ 546
PEGI 3
Diese App ist mit allen deinen Geräten kompatibel.
Installiert

Navigation
Messungen & Ergebnisse
Einstellungen
Online-Ergebnisse anzeigen
Feedback an cnlab senden
Änderungsprotokoll anzeigen
Über SpeedTest V2.4.3

Messung Ergebnisse Karte
Messort: --
Referenzserver: hel.blurwin.ch:80
Messdauer: ~30s
Messart: Einzelmessung
Letzte Messung
Download
Upload
Antwortzeit

Measurement 1.2 ...
7% Downloading ...
Speedometer and graph showing download and upload speeds over time.

Agenda

1. Informationssicherheit
2. Internet und Soziale Medien
3. Social Engineering (Angriffsbeispiele)
4. Massnahmen und Trends



SRF Einstein, 3. 9. 2015,
www.srf.ch/sendungen/einstein/cybercrime-wie-sicher-ist-das-know-how-der-schweiz

1. Informationssicherheit

Informationssicherheit: Was wollen wir schützen?

Information
(Asset, Value)

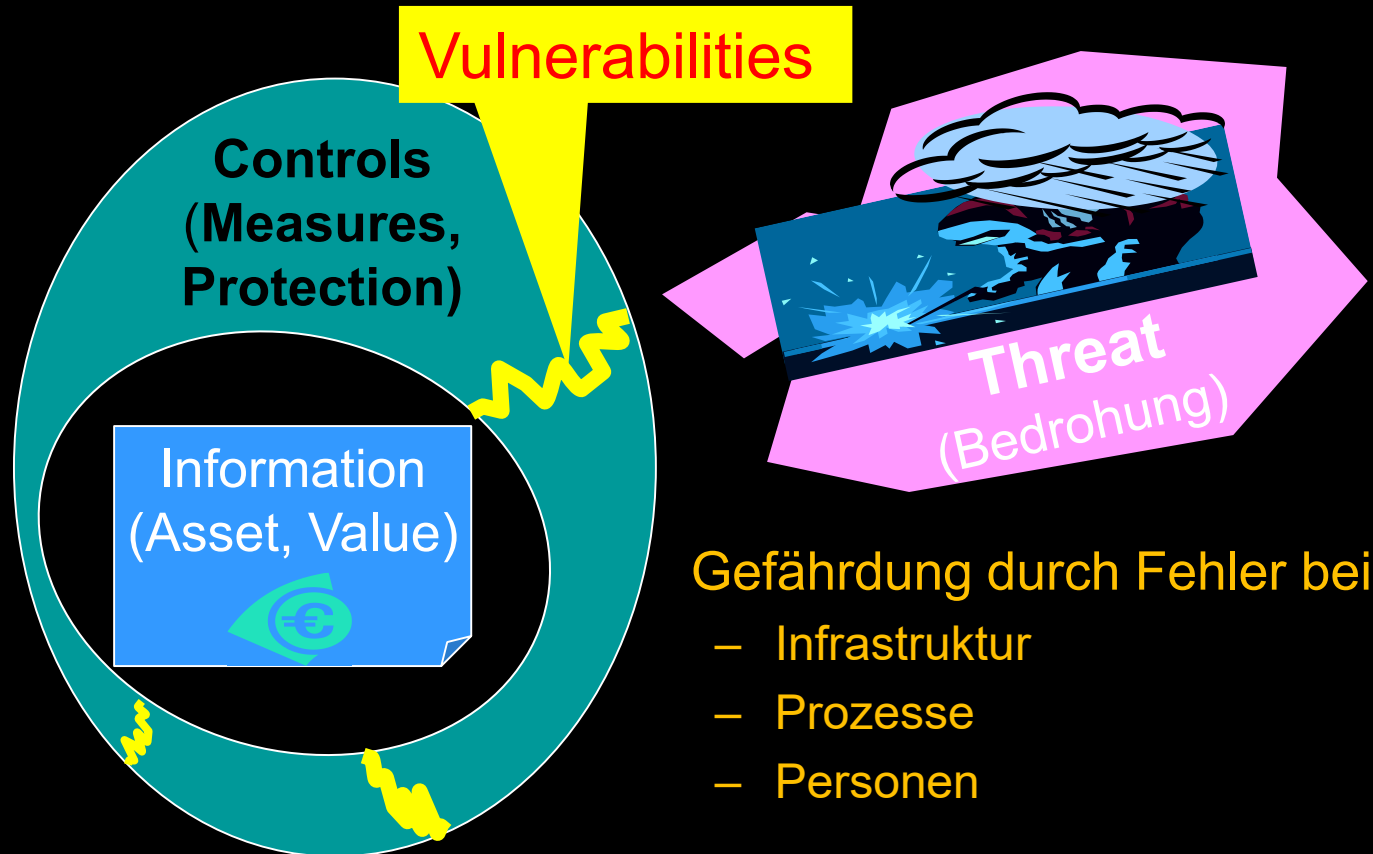


Informationssicherheitsmanagement

Management der Prozesse zur Aufrechterhaltung der Vertraulichkeit, Echtheit und Verfügbarkeit von Informationen

Schutz durch

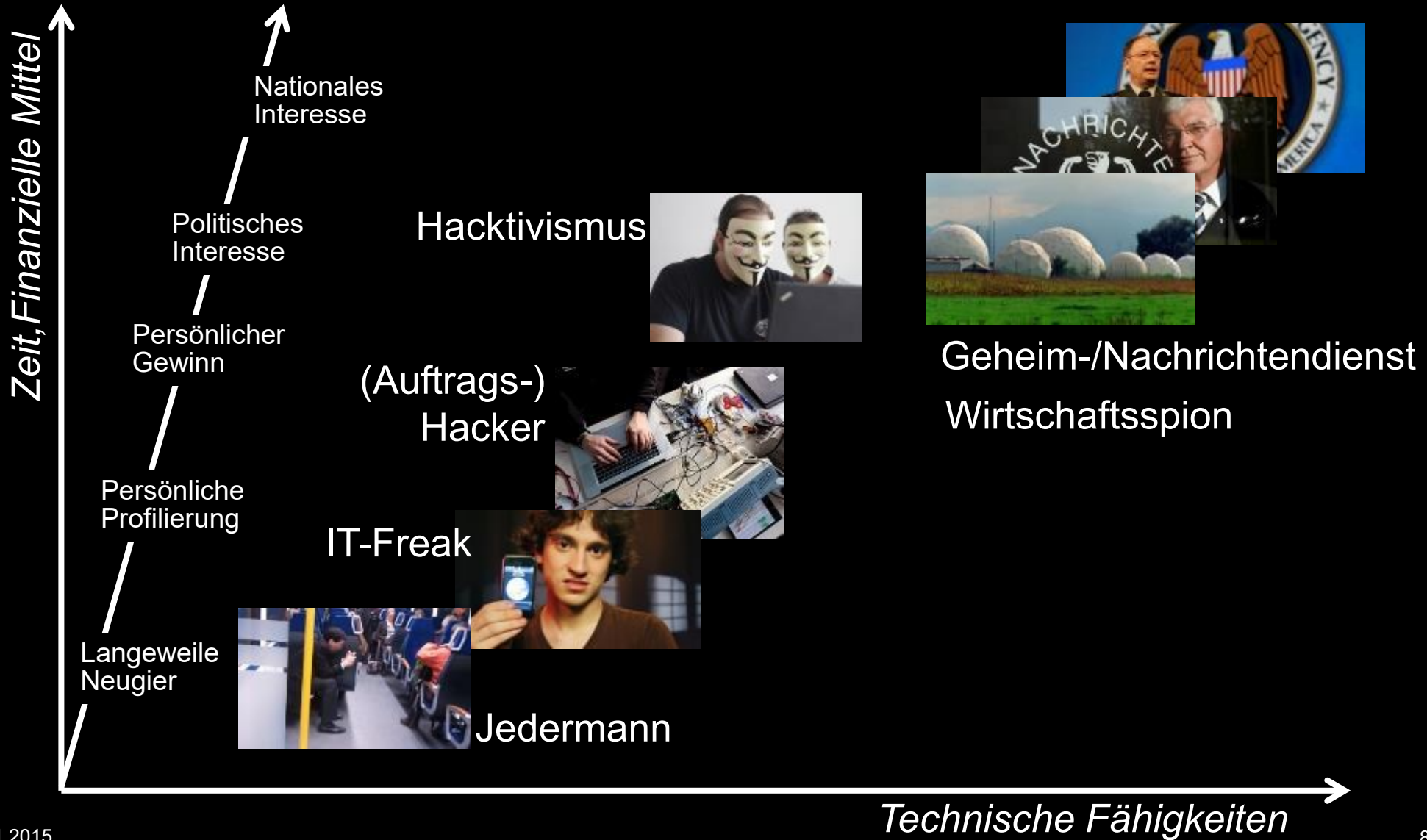
- organisatorische
 - technische
- Massnahmen



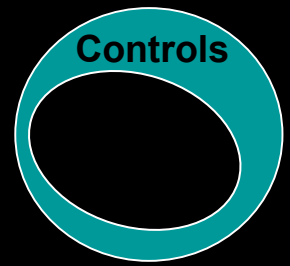
Gefährdung durch Fehler bei

- Infrastruktur
- Prozesse
- Personen

Gegen wen wollen wir uns schützen?



Wie sollen wir uns schützen?



	Problembereiche		
	Infrastruktur	Prozesse	Personen
Technische Massnahmen			
Organisatorische Massnahmen			

Welche Verletzlichkeiten gibt es?

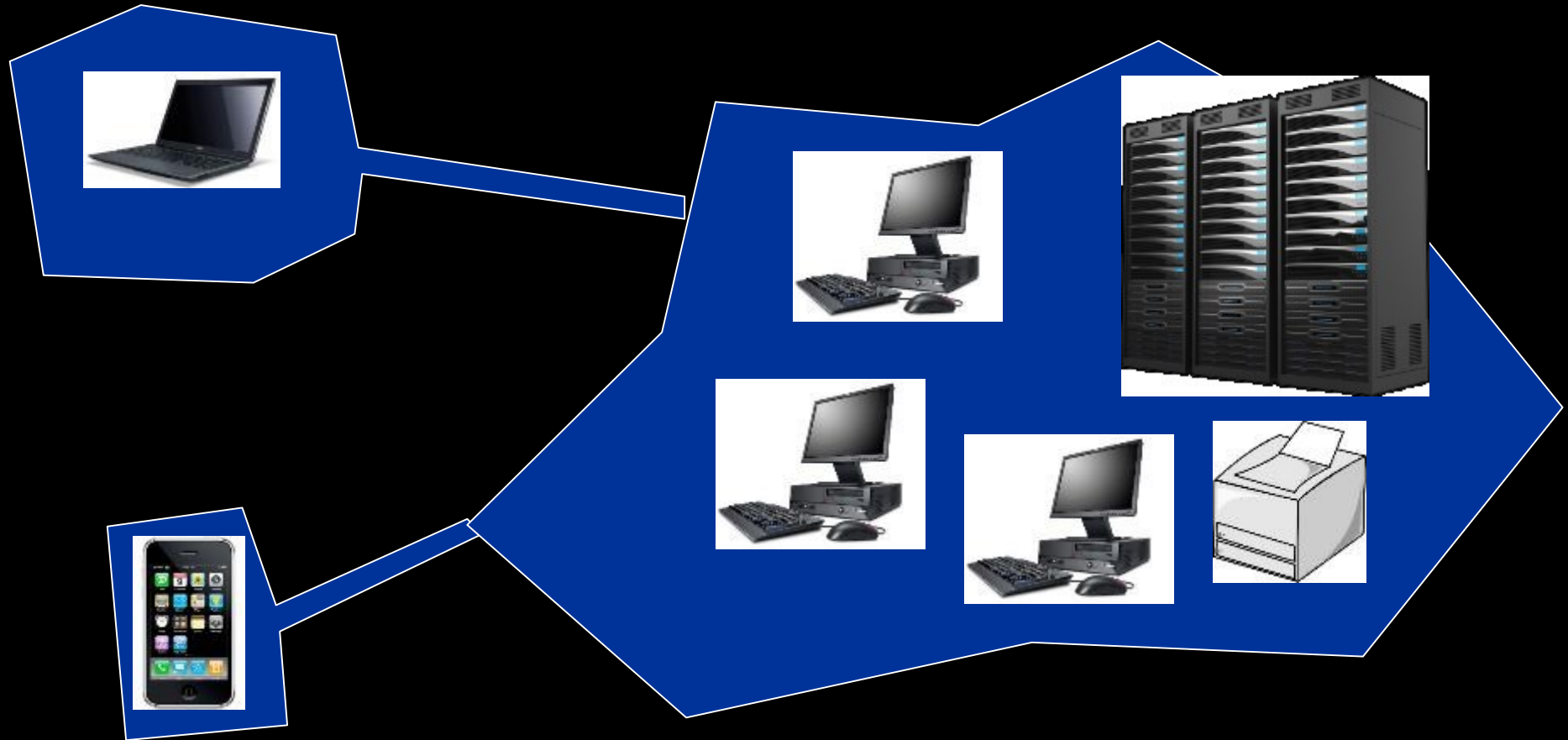


Infrastruktur

- www.shodanhq.com
- nvd.nist.gov
- www.osvdb.org
- www.exploit-db.com

Prozesse
Personen

«Technischer» Security Perimeter: IT und physische Sicherheit



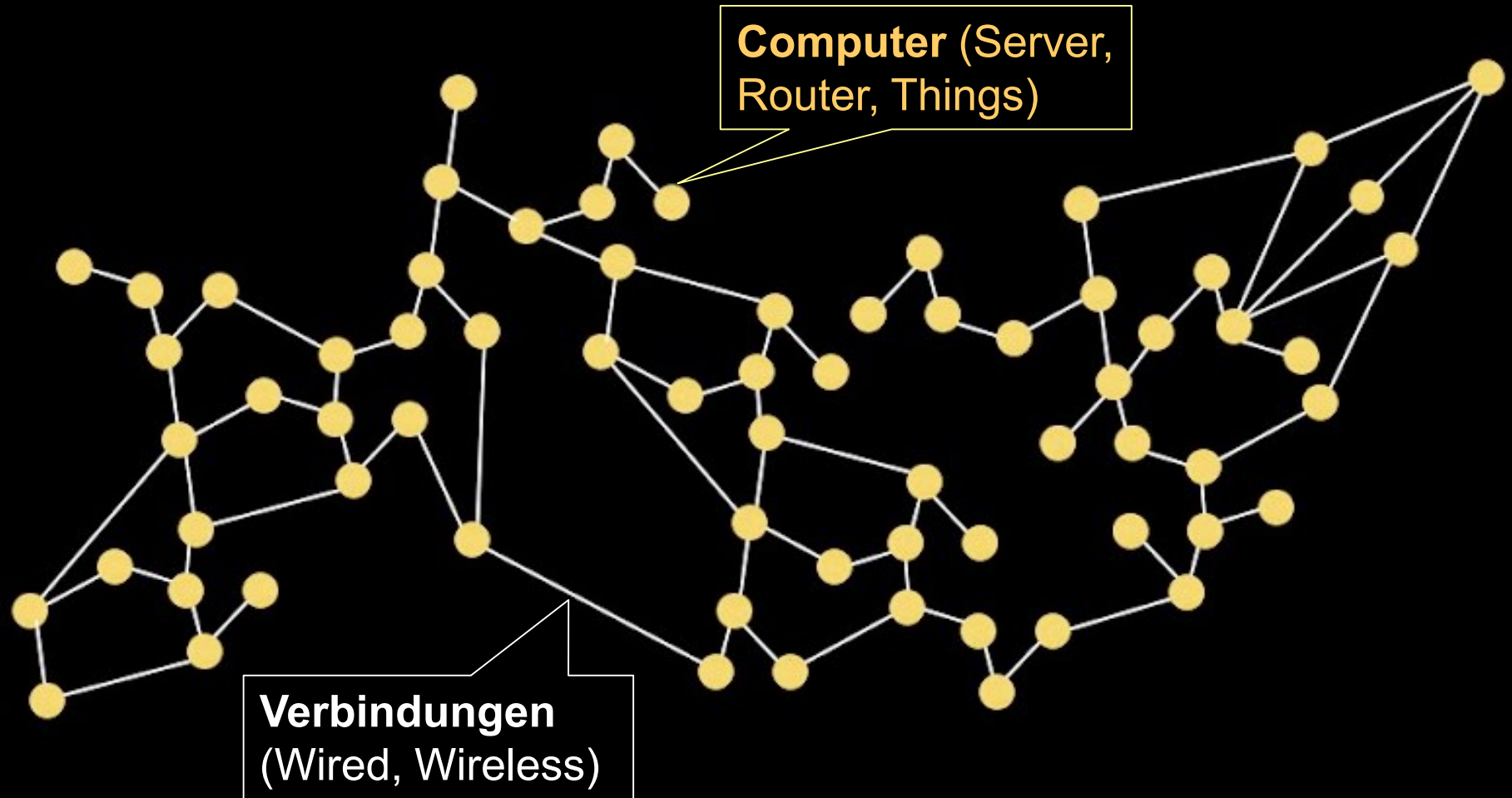
«Praktischer» Security Perimeter (Human Security Layer)



2. Internet und Soziale Medien zur Informationsbeschaffung

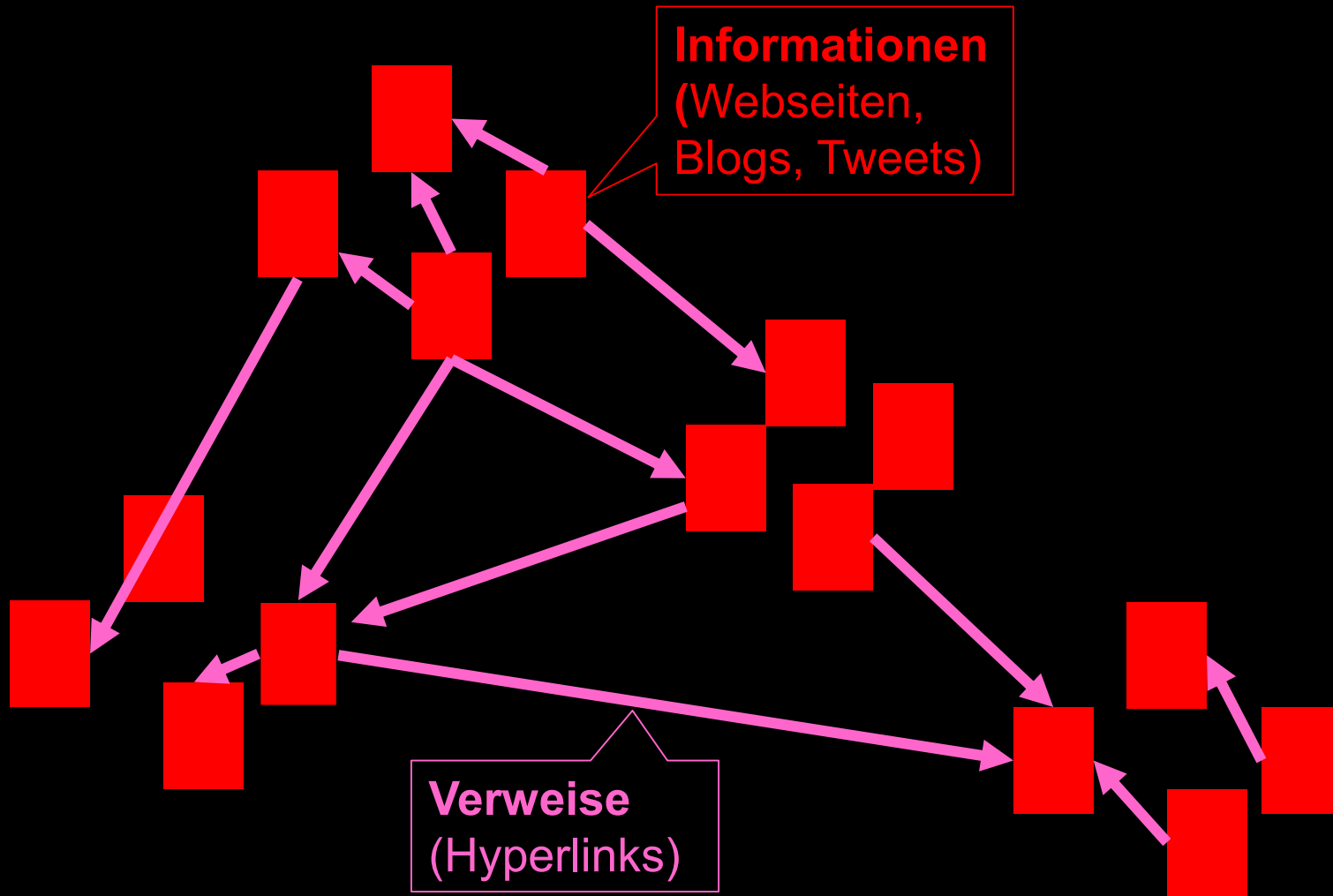
Internet of Computers

technische Vernetzung von Computern



Internet of Information

Vernetzung/Verweise zwischen Informationen



Was weiss das Internet über uns?

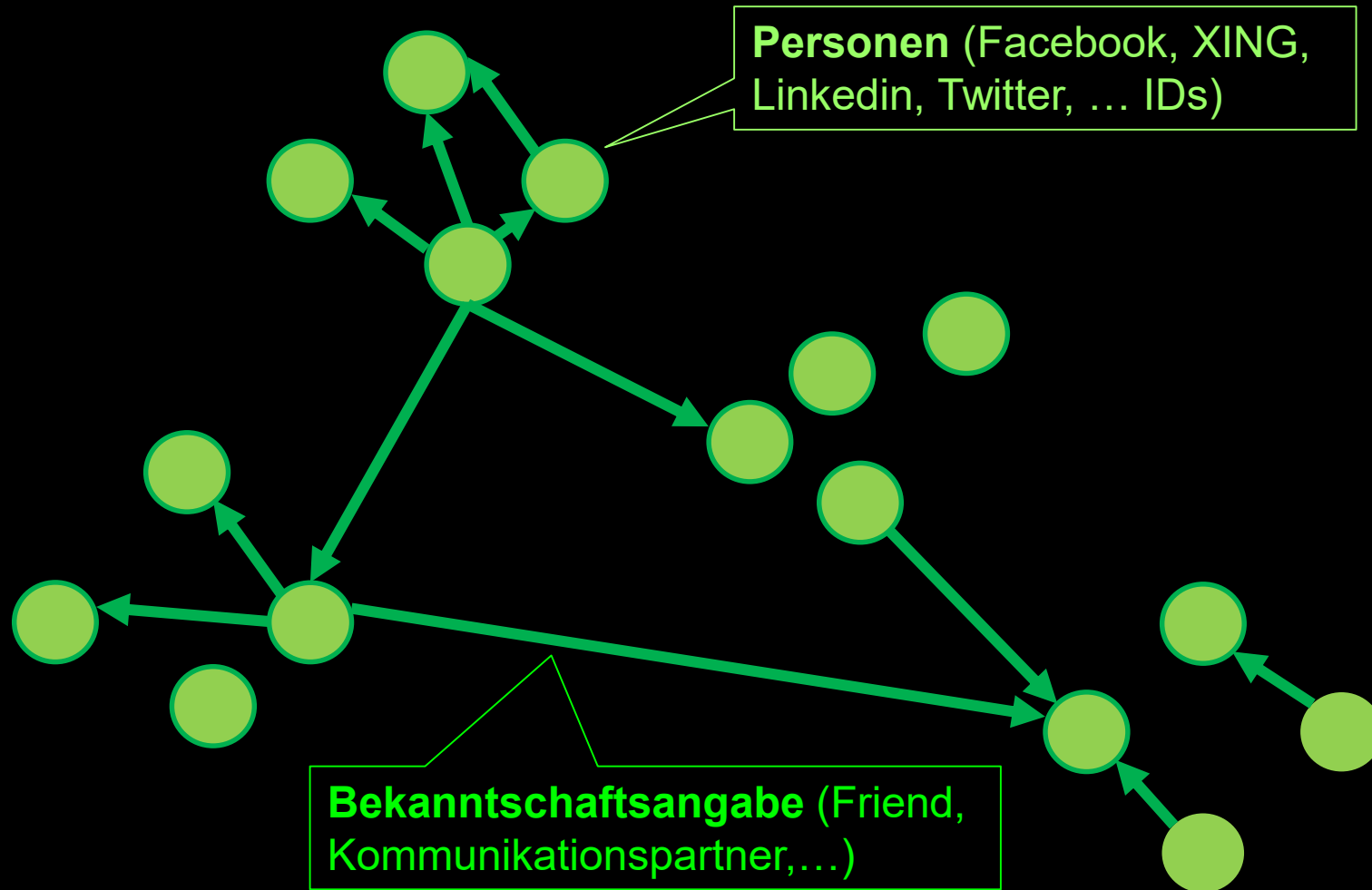


<https://www.youtube.com/watch?v=F7pYHN9iC9I>

https://www.youtube.com/watch?v=Rn4Rupla11M&src_vid=F7pYHN9iC9I&feature=iv&annotation_id=annotation_202513

Internet of People

Wer kommuniziert mit wem? Wer kennt wen? (Social Networks)



Personen Suchmaschinen

yasni[®] Tools Hilfe Produkte [+ Exposé schalten](#)

Peter Heinzmann Schweiz

Peter Heinzmann Person-Info für die Schweiz ([Ich bin Peter Heinzmann](#)) 345 Ergebnisse [Monitoring](#)

Es sind neue Ergebnisse zum Namen verfügbar. Hier klicken, um diese anzuzeigen >

[Marburg Windlach](#)

[Professor Hans-Peter Hochschule für Technik Hochschule Rapperswil Visperterminen Institut](#)
[Leiter Internet-Technologien CNLAB](#)

Bilder zu Peter Heinzmann (1 - 9 von 39 – alle anzeigen)

Eindeutige Personen

Peter Heinzmann, 60, Professor / Direktor @ cnlab AG / HSR Hochschule für
CNLAB Datenschutzbeauftragter ETH Hochschule Rapperswil Privacy Professor Rapperswil Switzerland Technik Themen

Branchenkontakte

Welche Firmen steuert **Peter Heinzmann**?

Sonstiges Geschäft **Peter Heinzmann:** Bdaino@fub.it, Branchenbuch von Meinestadt.de, Eyholz, Firmen, Routenplaner, Stadtplan, Visperterminen, Walligrundstrasse

Email zu Peter Heinzmann: peter.heinzmann@hsr.ch, peter.batchelor@ciid.dti.gov.uk, p.heinzmann@ostfildern.de

Veröffentlichungen allgemein

NZZ Online: Umfassende Insider-Information live von der Tour de...
www.presseportal.ch
Peter Heinzmann / René Vogt Tel.: +41 55 214 3330. E-Mail: info@tourlive.ch. Internet: www.nzz.ch · Banner medienjobs.ch · Logo NZZ Online ...

HSRWiki: Pruefungseinsicht Dozenten -
wiki.hsr.ch
Datum : Zeit : Raum : APF : Peter Sommerlad : siehe Prog3 : Bsys1 : Eduard Glatz : 1.10.17-18 : 6.112 : CN 1 :

Beispiele für DACH

www.yasni.ch

www.pipl.com

www.vebidoo.de

www.viadin.ch

www.persono.net

Fokus USA

www.webmii.com/

www.yourtraces.com

www.spokeo.com

www.zabasearch.com

www.peekyou.com

www.instantcheckmate.com

Soziale Medien

Major Social Networks	Blogging Sites	Location/Review Sites	Photo Sharing	Music Sites	Video Sites	Online Shopping
Facebook	Twitter	Formspring	Flickr	Pandora	dailymotion	Amazon
Google+	LiveJournal	Stumbleupon	Gravatar	Last.fm	Metacafe	eBay
Hi5	AOL Lifestream	CitySearch	Picasa	SoundCloud	Veoh	Etsy
Tagged	Blogger	Delicious	deviantART	Lyrics	YouTube	ThisNext
BlackPlanet	Tumblr	Eventful	Instagram		Break	Zazzle
Care2	WordPress	Foursquare	PhotoBucket	Dating	CNN iReport	Other Sites
Answers	Disqus	Pinterest	PictureTrail	Match	Vimeo	Ask.fm
Buzznet	Typepad	TripAdvisor	Behance	OkCupid		Github
Cafemom		Menuism	Fotolog	PlentyOfFish		SourceFor
IGN		Topix	SmugMug			

Gesamtheit der digitalen Technologien und Medien über die Nutzerinnen und Nutzer miteinander kommunizieren und Inhalte austauschen können.
stand 2013 erstmals im Rechtschreibbuden.

Kommt das Ihnen bekannt vor?

- Ich war vor 11 Monaten im Hotel Babalou in Paris, Frankreich.
- 2012 hatte ich eine Canon EOS 5D Mark II.
- Am 6. Februar 2015, 15:11 war ich an einem Workshop in ...
- Im März 2015 war ich in Budapest
- Ich schaue regelmässig YouTube Videos.
- Groß-Gerau und Darmstadt kenne ich gut.
- Ich habe im Juni 2015 geheiratet.
- Ich gehe gerne zu Starbucks.



Spokeo

SPOKEO robert.schwerdtner@telekom.com

1 Username Match

63+ Social Media Platforms Searched

- Amazon, Facebook, Messenger, Google+, SoundCloud, LinkedIn
- Pinterest, Instagram, Tumblr, Twitter, Ask, Email
- Classmates, Facebook, Email, Dribbble, A, ...
- eBay, Twitter, cm, Dm, Dribbble
- 7, ebay, E, e, P, ...
- Google, Instagram, OS, m, ...
- ... , .p, POF, ...
- ... , t, weah, WP, YouTube, B6
- ... , i, D, ... , K
- L, ... , sf, tn, t
- ... , v, e

We Found a Possible Match!

robert.schwerdtner@telekom.com

✓ 1 Social Networks ✓ 3 Photos and Videos

Tweet

1 Username Match for *robert.schwerdtner* †
We Searched 63+ Networks

Robert Schwerdtner
Picasa

The collage consists of three distinct images: a group of people sitting together, a high-contrast close-up of a man's face, and a colorful roller coaster at a theme park.



Picasa

Picasa™ Web Albums

Home My Photos Explore Robert Schwerdtner's Gallery

Robert Schwerdtner's Gallery Albums (2) Sort by: Album date ▾

Share

 Profile Photos
Feb 6, 2015
photos: 2

 Scrapbook Photos
Jul 26, 2011
photos: 1

Robert Schwerdtner photos
+8 Follow
RSS

©2011 Google [Terms](#) - [Download Picasa](#) - [Privacy Policy](#) - [Developer](#) - [Blog](#) - [Google Home](#)



Facebook

Facebook interface showing a user profile for Rob Schwerdtner. The profile picture is a man drinking from a large beer mug. The page includes navigation tabs (Chronik, Info, Freunde, Fotos, Mehr), a "KENNST DU ROB?" section with a "Freund hinzufügen" button, and a "FOTOS" gallery. A recent post shows the user updating their profile picture to the same man drinking from a beer mug.

Rob Schwerdtner

Freund hinzufügen Nachricht senden

Chronik Info Freunde Fotos Mehr

KENNST DU ROB?

Um zu sehen, was er mit Freunden teilt, sende ihm eine Freundschaftsanfrage.

Freund hinzufügen

Arbeitet bei Konzerlagezentrum
1. November 2012 bis heute

Sein Arbeitsjubiläum war vor 4 Tagen
Hat 2012 begonnen


FOTOS

Rob Schwerdtner hat sein Profilbild aktualisiert.
3. Oktober

Deutsch · Datenschutz · Impressum · Nutzungsbedingungen · Cookies · Werbung




Google+



Robert Schwerdtner
Arbeitet bei Deutsche Telekom
Hat gewohnt in Cottbus

[+ Zu Kreisen hinzufügen](#)




22 Follower | 159.185 Aufrufe




Über mich | Beiträge | Foto | Videos | Bewertungen

Personen

In den eigenen Kreisen 50 Personen

-  Tanja Djordjevic [+ Hinzufüg...](#)
-  Friedemann von Winterfell [+ Hinzufüg...](#)
-  Pia K [+ Hinzufüg...](#)

In Kreisen von anderen 22 Personen



Arbeit

Beschäftigung

Deutsche Telekom
2004 - heute


Allgemeine Informationen

Geschlecht Männlich

Geschichte

Motto
"A great photograph is one that fully expresses what one feels, in the deepest sense, about what is being photographed." Ansel Adams

Orte





©2015 Google | Map data ©2015 GeoBasis-DE/EG (©2009), Google

Vorher

Cottbus - Bischofsheim - Weiterstadt - Bonn - Geseke

Links

YouTube
 Robert Schwerdtner





Robert Schwerdtner

[Abonnieren](#) 0

[Übersicht](#) [Videos](#) [Playlists](#) [Kanäle](#) [Diskussion](#) [Kanalinfo](#) [Suche](#)


Alle Aktivitäten ▾


 Robert Schwerdtner hat einen Kanal abonniert. vor 1 Woche




hyperboleTV
444 Videos
Wir übertreiben. Nein, wirklich. Eine Hyperbel ist die literarische Form der Übertreibung, um einen Sachverhalt zu verdeutlichen. Wir wollen politische Themen so interessant erzählen,...


[KANAL](#) [Abonnieren](#) 69.410


 Robert Schwerdtner hat ein Video positiv bewertet. vor 3 Wochen



Darf ich Nazis verpetzen? | Kanzlei WBS
von Kanzlei WBS
vor 3 Monaten • 18.510 Aufrufe
Darf ich Nazis bei deren Arbeitgeber verpetzen? Oder darf ich Kommentare von ihnen online veröffentlichen? Wir klären es in diesem Video....

 Robert Schwerdtner hat ein Video positiv bewertet. vor 4 Wochen



Street Portrait Photo How To
von WIRED 
vor 6 Jahren • 134.588 Aufrufe
Photographer Clay Enos goes from shooting super heroes on the set of Watchmen to taking random street portraits. He shows us how to do a street-studio portrait session with a sheet...

Robert Schwerdtner

Social Media Crisis Manager

👍 + ➔ Email Me

Schwerdtner, Robert

Menschen lieben es zu kommunizieren. Menschen müssen gar kommunizieren. Getreu dem Zitat von Paul Watzlawick, "Man kann nicht nicht kommunizieren", bin ich der Überzeugung das dieses Grundbedürfnis der Grundstein des Social Web ist. Das Social Web wird also bleiben und wir alle müssen lernen damit umzugehen. Ich bin ebenso der Überzeugung das wir noch viel Nachholbedarf im Umgang mit diesem Medium haben.

Genau darum geht es bei Digital Acceleration, wir versuchen uns dieser Herausforderung zu stellen.

Nun zu mir. Ich bin Notfall- und Krisenmanager, im Konzernlagezentrum der Deutschen Telekom AG verantwortlich für die Integration verschiedenster Social Media Thematiken. Ich beziehe meine Erfahrung aus meiner fachlichen Spezialisierung unter anderem in den Bereichen Datenschutz (UDIS), Social Media Management (MC), Projektmanagement (IPMA) sowie Krisenmanagement (CECM.). Referent zu den Themen Social Media Nutzung, Monitoring und Recht. Mein Ziel ist es die Thematiken Social Media oder besser Digital Crisismanagement und Social Media Risk/Security Monitoring zu prägen und zu gestalten denn ein modernes Lagemanagement kann Geld, Reputation uns sogar Leben retten!





XING

XING Suchen Sie nach Jobs, Kontakten, Events ... Erweiterte Suche Neue Kontakte finden Hilfe

Robert Schwerdtner Jetzt Premium-Mitglied werden! Mehr Infos

Prof. Dr. Peter Heinzmann > Nhung Truong > Alexander Luyken > Robert Schwerdtner Alle Verbindungen

Prof. Dr. Peter Heinzmann BASIS

- Meine Startseite
- Meine Kontakte 7
- Meine Nachrichten 2
- Premium-Bereich
Jetzt Premium-Mitglied werden!
- Stellenmarkt
- Events 1
- News NEU
- Gruppen
- Unternehmen
- Projekte
- Für Unternehmen
- Weitere Services

Robert Schwerdtner PREMIUM

Experte Notfall und Krisenmanager Schwerpunkt Social Media
Deutsche Telekom AG Bonn, Deutschland
Angestellter

301 Kontakte 90% Aktivität 0 Gemeinsamkeit

Als Kontakt hinzufügen
Nachricht schreiben
Kontaktdaten mehr

Meine Notizen zu Robert Schwerdtner

Ich biete

- Social Media Management Krisenmanagement Projektmanagement (IPMA) Datenschutz (UDIS)
- Kommunikation Digitale Geschäftsmodelle New Business Development Konzeptentwicklung
- Consulting IT-Consulting eLearning WBT Aus- und Weiterbildung digitale Bildbearbeitung
- kreatives Denken Telekommunikation Telekommunikationsrecht Internetrecht Arbeitsrecht
- Social Media Social Networking Social Skills Projektmanagement BCM
- Veranstaltungsplanung Veranstaltungsorganisation Social Media Monitoring

Berufserfahrung

07/2014 - heute
Experte Notfall und Krisenmanager Schwerpunkt Social Media
Deutsche Telekom AG
www.telekom.com

Profildetails

Portfolio

Weitere Profile im Netz

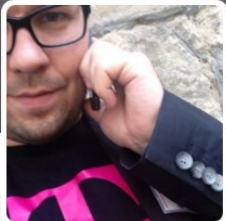
Kontakte

Events



Twitter

Home Notifications Messages Search Twitter Tweet




Rob Schwerdtner
@RobertSchwer

a man with many dreams and a job as digital crisis manager and data analyst
[@DeutscheTelekom](#)

Bonn
[ridtulous.com](#)
Joined March 2011

[Tweet to Rob Schwerdtner](#)


98 Photos and videos



TWEETS 687 FOLLOWING 95 FOLLOWERS 205 LIKES 486 LISTS 4 [Follow](#)

Tweets Tweets & replies Photos & videos

Rob Schwerdtner Retweeted **Datentreiber** @Datentreiber · 12h
DT Wacken-Fans haben skn höheres Datenschutzbewußtsein als Oktoberfest-Besucher. [@RobertSchwer](#) auf der #pawcon



4 8

Rob Schwerdtner @RobertSchwer · Nov 2
Hi [@NattyHammes](#) natürlich bringe ich euch ein paar Beispiele mit!
[@Unperfekthaus](#) [@bloggerabc](#)

1 View conversation

Rob Schwerdtner Retweeted **Daniela Sprung** @bloggerabc · Nov 2
Heute Abend im [@Unperfekthaus](#) SoMe Stammtisch! Thema: Krisenkommunikation in Zeiten sozialer Medien. Mit Sicht aus der Telekom.

Who to follow · Refresh · View all

- [Twitter](#) @twitter [Follow](#)
- [Guardian Tech](#) @guardian... [Follow](#)
- [Jacob Rudenstam](#) @jruden...
Followed by Bo Rickard [Follow](#)

Find friends

Trends · Change

- Arsenal
- Bayern
- #TheApprentice
- #MOBOAWARDS
- Willian
- #sfrundschau
- Robben
- #10vor10
- Zurich
- #JourTag15

© 2015 Twitter About Help Terms Privacy Cookies Ads info



LinkedIn

Robert Schwerdtner
Experte bei Deutsche Telekom AG
Köln und Umgebung, Deutschland | Telekommunikation

Früher Deutsche Telekom
Ausbildung Facilitation - Kommunikationslotsen

[InMail an Robert Schwerdtner senden](#) 225 Kontakte

<https://de.linkedin.com/in/robert-schwerdtner-b7597251>

Über mich

Berufserfahrung

Experte
Deutsche Telekom AG
Juli 2014 – Heute (1 Jahr 5 Monate)

emergency and crisis management; social media expert; social media crises, social media community manager, travelsecurity

- ▶ 1 Projekt
- ▶ 1 Organisation

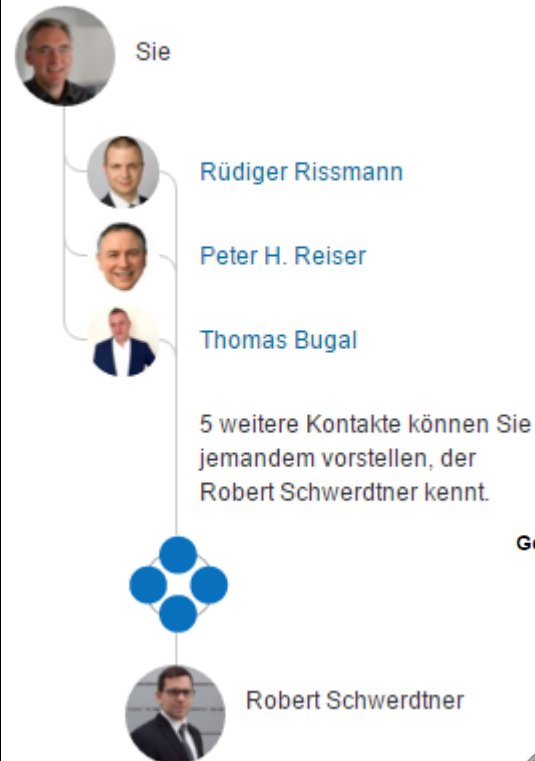
Referent
Deutsche Telekom
November 2012 – Juli 2014 (1 Jahr 9 Monate)

emergency and crisis management; social media expert, social media community manager, travelsecurity

Geschäftsführung Konzernauszubildendenvertretung
Deutsche Telekom
Februar 2008 – November 2012 (4 Jahre 10 Monate)

negotiation, talentmanagement, IT systems, internship/training concepts

Sehen Sie, wie Sie miteinander verbunden sind



Gemeinsam mit Robert Schwerdtner



3. Social Engineering

Social Engineering beschreibt die zwischenmenschliche Beeinflussung von Personen mit dem Ziel, bei diesen Personen bestimmte Verhalten hervorzurufen.

socialis (lat): kameradschaftlich, gesellig, Synonym zu „gesellschaftlich“ und im erweiterten Sinn zu „gemeinnützig, hilfsbereit, barmherzig“

Ablauf von Angriffen

(Penetration Test auf Infrastruktur oder Personen)

Angriffsstrategie:
Zielsetzung

Informationsbeschaffung:
Umfeldanalyse

Informationsbeschaffung:
Zielbeobachtung

Angriffsauslösung:
**Direkt / indirekt via
Infrastruktur, Prozesse,
Personen**

Engineering von Angriffen



- Ingeniör
- ingenium (lat)
 - Erfindung, Scharfsinn, Kriegsgerät,
 - angeborene Fähigkeit, natürlicher Verstand, Scharfsinn, Begabung
 - schöpferischer Geist, Genie, Talent
- Berufs- bzw. Standesbezeichnung für Fachleute bzw. Experten auf dem Gebiet der Technik

Wieso reagieren wir auf Aufforderungen anderer Menschen?

- Weil wir sie gut kennen, Arbeitskollegen, Freunde
- Aus Respekt vor Autoritäten (Uniformierte, Chefs, Bekannte)
- Wegen Aussichten auf finanzielle Vorteile, Vergünstigungen, Gewinn
- Aus Neugier
- Aus Höflichkeit, Hilfsbereitschaft, Helferinstinkt
- Aus Interesse an Personen (attraktiv, interessant, prominent, kompetent, bekannt)
- Um Hilfe zu erhalten
- Weil wir in speziellen Situationen oder unter Druck sind, Stress
- Aus Gewohnheit
- Um Anerkennung zu erhalten
- Um dazu zu gehören
- ...

Malware-Verteilung

Neugier, finanzielle Anreize, Vergünstigung



CDROM, USB-Stick, Human Interface Devices (HID) und weitere Gadgets



- Keyboard & Refreshable braille display
- Pointing devices: Mouse, Trackball, Touchpad, Pointing stick, Light pen
- Touchscreen
- Magnetic Stripe Reader
- Graphics tablet
- Joystick, Gamepad, Analog stick
- Webcam
- Fingerprint Scanner

Phishing

Nach Analysen von IT-Sicherheitsdienstleistern beginnen zwischen 70% und 90% aller Cyber-Attacken mit infizierten Mails.

Damit sich die Empfänger angesprochen fühlen, werden die Mails optimal auf die Adressaten angepasst (Spear Phishing).

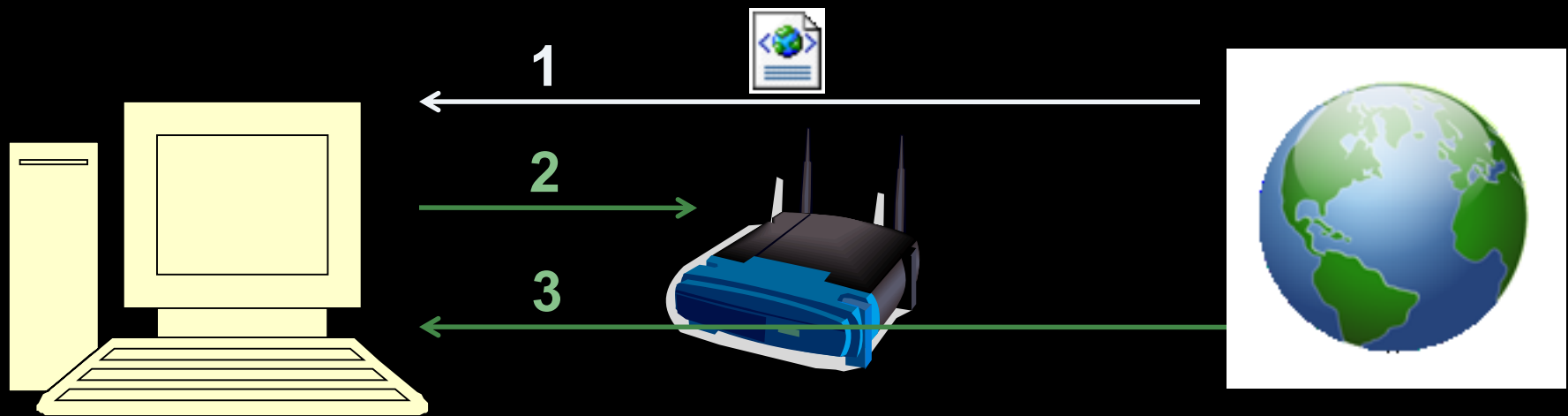
Vertrauensbildung: Anpassen, Einschmeicheln, Einschleimen



Beispiel: Drive-by-Download

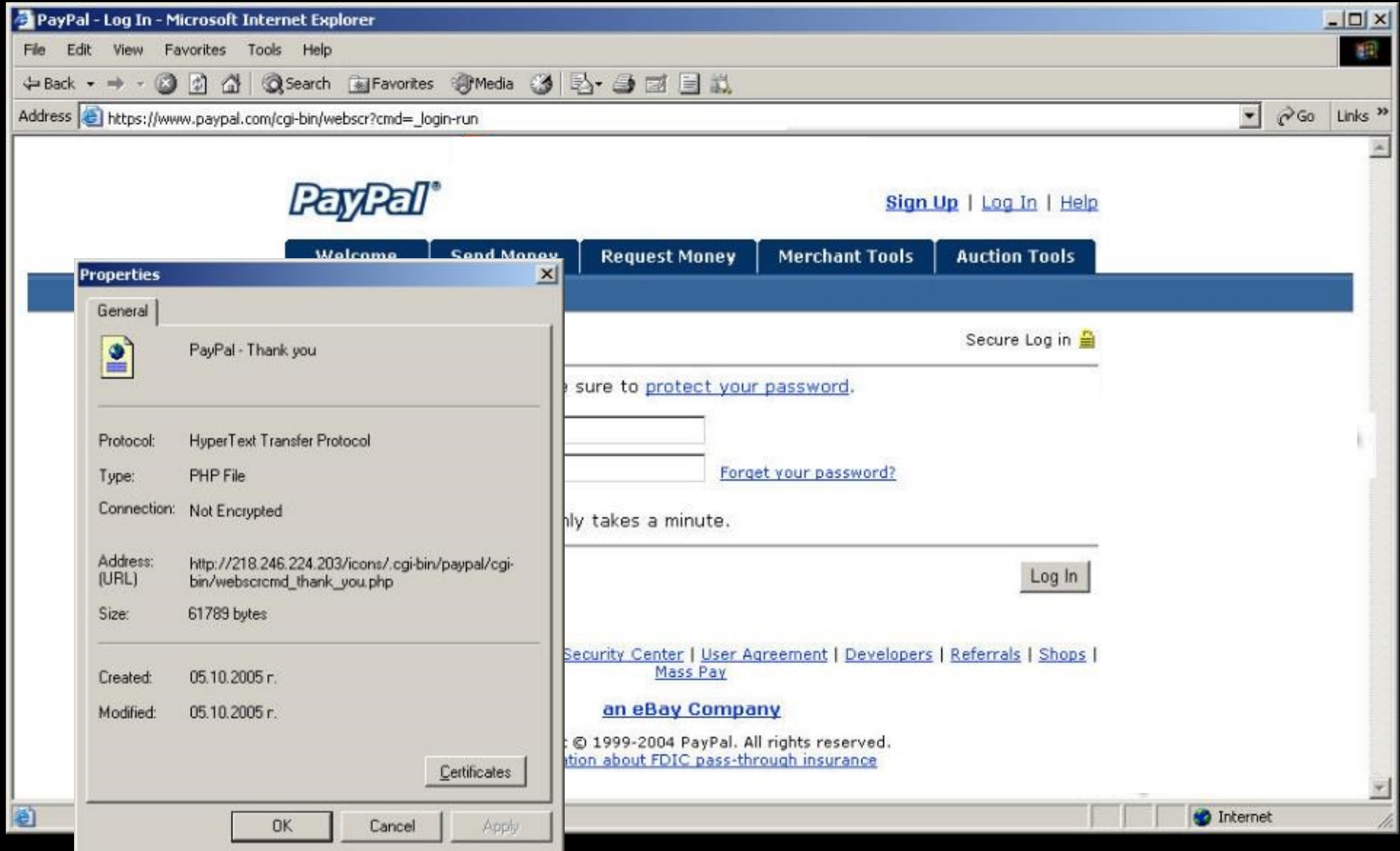
- Unbewusstes Herunterladen und ausführen von Programmen (Malware)
 - beim blossen Aufruf von Webseiten
 - bei blosser Betrachtung einer E-Mail
 - bei blosser Betrachtung von Dokumenten
- Nutzt Verletzlichkeiten von
 - Browsern und Browser Zusatzprogrammen (Plugins)
 - Anwendungen

Drive-by-Download: Inside-Out Attacke auf Router



https://192.168.1.1/apply.cgi?submit_button=Firewall&change_action=&action=Apply&block_wan=1&block_loopback=0&multicast_pass=0&ident_pass=0&block_cookie=0&block_java=0&block_proxy=0&block_activex=0&filter=off&_block_wan=1&_block_multicast=0&_ident_pass=1

Übung: Phishing Quiz



<https://phishingquiz.mcafee.com/>

Kali Linux Social Engineering Toolkit (SET) Basic Hack

```
root@kali: ~  
File Edit View Search Terminal Help  
[---] Homepage: https://www.trustedsec.com [---]  
  
Welcome to the Social-Engineer Toolkit (SET).  
The one stop shop for all of your SE needs.  
  
Join us on irc.freenode.net in channel #setoolkit  
  
The Social-Engineer Toolkit is a product of TrustedSec.  
  
Visit: https://www.trustedsec.com  
  
Select from the menu:  
  
1) Social-Engineering Attacks  
2) Fast-Track Penetration Testing  
3) Third Party Modules  
4) Update the Metasploit Framework  
5) Update the Social-Engineer Toolkit  
6) Update SET configuration  
7) Help, Credits, and About  
  
99) Exit the Social-Engineer Toolkit  
set>
```

Similar Names und Homograph Attacks

- Registrierung von Domänen die ähnlich aussehen wie die anzugreifende Domäne
 - «TypoSquatting» nutzt Schreibfehler im URL
 - Testanwendung <http://paderbutze.de/typosquatting/>
 - «Homograph Attack» ersetzt URL-Zeichen durch ähnlich oder gleich aussehende Zeichen
 - Verwendung von ähnlich aussehenden Zeichen l=I, O=0, rn=m, ... (z.B. www.PayPal.com, www.rmicrosoft.com, www.G00GLE.COM, www.appenzeller.ch)
 - Verwendung von International Domain Name (IDN) Zeichen, welche in anderen Sprachen gleich aussehen (confusables.txt) (z.B. www.amazon.com, www.irs.com)


<http://paderbutze.de/typosquatting/>

TypoSquatting

Wer will denn da schon wieder was abgreifen?

Domain:

Layout: Deutsch Englisch

Gefunden:  36%

Domain	IP	Info
deutschebank.de	160.83.8.78	Denic
<i>Taste vergessen</i>		
eutschebank.de ☼	185.53.177.6	Denic
dutschebank.de ☼	103.224.182.245	Denic
detschebank.de ☼	72.52.4.119	Denic
deuschebank.de ☼	185.53.177.7	Denic
deutchebank.de ☼	keine ip	Denic
deutshebank.de ☼	keine ip	Denic
deutschebank.de ☼	72.52.4.119	Denic
deutschbank.de ☼	185.53.179.6	Denic
deutscheank.de ☼	103.224.182.239	Denic
deutschebnk.de ☼	103.224.182.243	Denic
deutschebak.de ☼	keine ip	Denic
deutscheban.de ☼	72.52.4.90	Denic
<i>Tasten vertauscht</i>		
edutschebank.de ☼	kein dns	Denic
duutschebank.de ☼	185.53.178.9	Denic
detutschebank.de ☼	185.53.179.8	Denic
deustchebank.de ☼	185.53.177.6	Denic

Social Media Attacke

- Wie reagieren Sie, wenn Sie von Ihrem Freund Felix Muster eine E-Mail erhalten mit der Absenderadresse felix.muster@gmx.net ?
- Wie reagieren Sie, wenn Sie von einem Geschäftspartner eine Social Media Kontaktanfrage erhalten?

Passwort Bekanntgabe

Neugier wecken, verwirren, spezielle Situation



spezielle Situationen, Druck, Stress



<https://www.youtube.com/watch?v=opRMrEfAlil#t=77> (2min49)

Respekt vor Autoritäten (Uniformierte, Chefs, Bekannte, Interner Helpdesk Mitarbeiter)

- «SF Spezial»: «Alles unter Kontrolle?»
 - Mitarbeitende des Schweizer Fernsehens überlassen ihr Passwort einem mutmasslichem Helpdesk-Mitarbeiter
 - Aktion ist dokumentiert mit versteckter Kamera



Physischer Zugang

Gebäude-/Raumzutrittskontrolle (Sicherheitsschleuse)



- Identifikation der Person
 - What you know
 - Geheimcode
 - What you have
 - Badge (Magnetstreifen, RFID, NFC Mobile)
 - What you are
 - Iris-Scan
 - Hand-Scan
 - Fingerabdruck
 - Gewichtskontrolle

Umgehung der Zutrittskontrolle



- Auftritt als
 - Service Techniker
 - Reinigungspersonal
- Einlass durch Mitarbeitende
 - Mit viel Gepäck vorm Eingang
 - Mit oder ohne Badge anderen folgen
- Tailgating, Piggybacking
- St. Nikolaus Angriff

4. So what?

Massnahmen und Trends

Massnahmen

- Sensibilisierung der Mitarbeiter:
Wachsamkeit, «gesundes Misstrauen» fördern
 - Gefälschte Absender (bei E-Mail, SMS/Telefon und Social Media)
 - Unbekannte abweisen, Glaubwürdigkeit überprüfen (Rückfragen oder Rückruf)
- spontane Reaktionen vermeiden:
bedächtig reagieren, Zeit verschaffen (soziale Automatismen ausschalten)
- Nicht nur Eintritt sondern auch Austritt aus der Firma kontrollieren (Austritt nur mit gültigem Badge)
- «Fehler» von Mitarbeitenden mit technischen Massnahmen abfangen

Trends

- «Advanced Persistent Threat (APT)» wird zum Standard Angriffsszenario
 - Blended
 - Cybercrime/Phishing as a Service
 - Internationalisierte, professionelle Wertschöpfungsketten
- «Internet der Dinge» wird auch bei Social Engineering Angriffen genutzt werden
- «Mental Firewall» und «Person Hardening»

Bewerbung als Marketing-Managerin

Sehr geehrte Frau [REDACTED]

Aus familiären Gründen werde ich in Kürze ins Appenzellerland ziehen und würde die Sortenorganisation bei Käse sehr gerne als Marketing-Managerin unterstützen.

Aktuell arbeite ich als Marketing-Managerin im Bau- und Verkehrsdepartement in Basel im ungekündigten Arbeitsverhältnis und schätze die abwechslungsreiche Tätigkeit in der Marketingabteilung. Meine derzeitigen Aufgaben sind hauptsächlich in den Bereichen Recruiting und Entwicklung und Evaluierung von Online-Marketingstrategien angesiedelt.

Meinen Kompetenzen und Stärken sind nebst meiner mehrjährigen Berufserfahrung Zuverlässigkeit, Fleiss und eine rasche Auffassungsgabe.

Bitte werfen Sie doch einen Blick auf meinen beigefügten Lebenslauf:



So liessen sich beispielsweise folgende Informationen beschaffen:

- Ausbezahlte Provisionen bei richtigem Fett- und Wassergehalt
- Bilanz des letzten Jahres
- Lohnausweise
- Passwortliste in Excel File

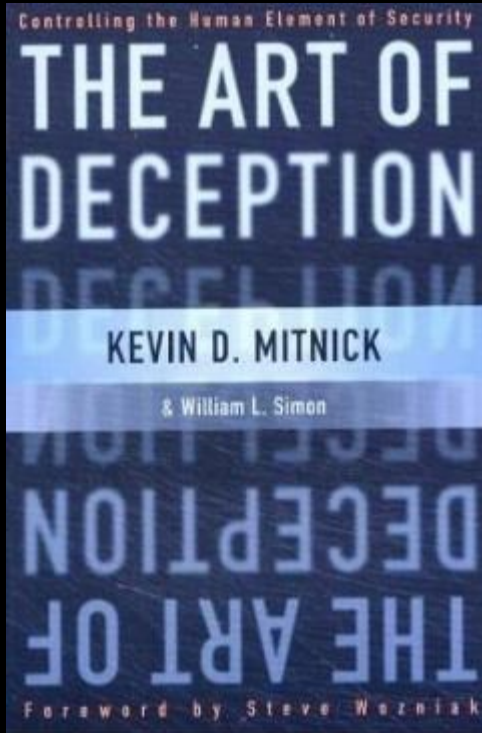
... und wo ist das geheime Rezept zum Appenzeller Käse?



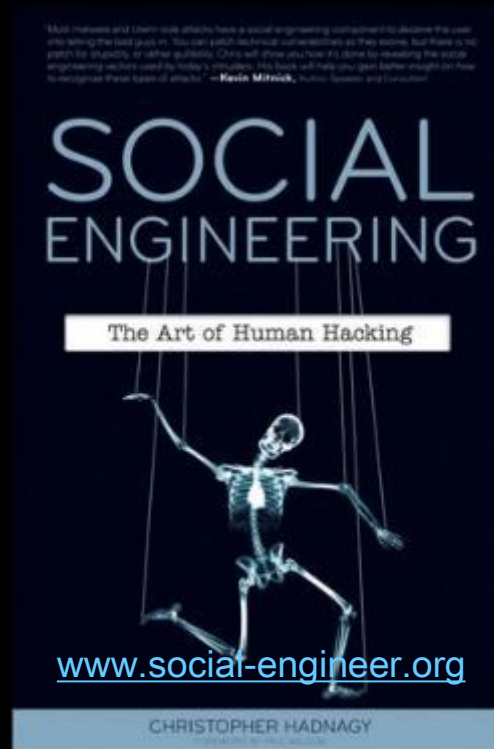
Weitere Infos bei www.cnlab.ch



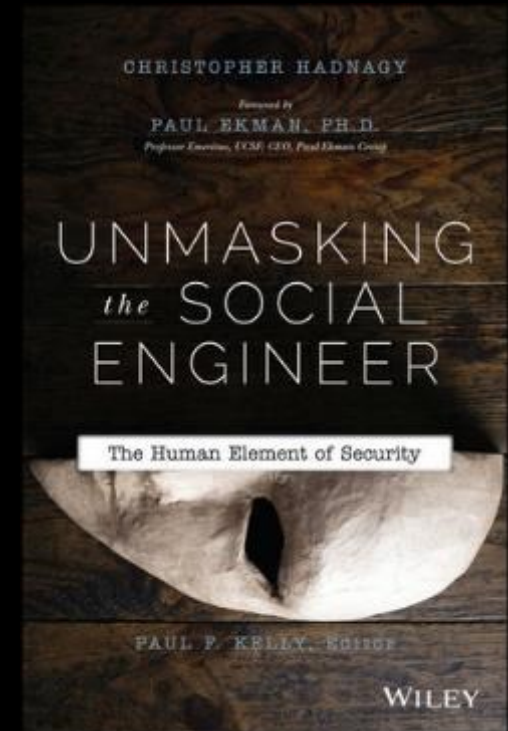
Social Engineering



Controlling the Human Element of Security, 2002



The science of influencing a target, 2010



How to detect the social engineer, 2014

TREsPASS Social Engineering Challenge

- Security Nightmare 2015 – Cloud Attack!
 - attack scenarios for a cloud-based setting



- TREsPASS: Social Engineering Challenge 2014 Think of a new Social Engineering attack idea and a suitable countermeasure to prevent your scenario from taking place
 - company workers are sought out on their charity involvement and are time-pressured into (unwittingly) installing malware on the network
 - targeting people’s curiosity or wallet, but rather their heart, identity and sense of responsibility.
 - Besides strict technical measures, the company should strengthen its selection process, enforce permanent awareness and perhaps maintain online honeypots.