

# Der Mensch im Fokus – als Risiko aber auch als Chance

Michael Lardschneider, CISO

IHK – (IT)-Sicherheit aus Unternehmenssicht  
München, 25.06.2008



Münchener Rück  
Munich Re Group



31.1.1983 Werkstudent

1984 Lehre zum Versicherungskaufmann

1986 Einbruchdiebstahl- und Raubversicherung

1989 Wechsel in die EDV (Helpdesk)

1991 Virenschutzbeauftragter (MRM)

1994 Sicherheitsbeauftragter (MRM)

1997 Leiter des int'l Projekts *@lcatraz* (MRV)

1999 CISO (MRV)

2005 Mitglied im GISC (MRV)

2008 Leiter GSCM (MR Gruppe)



*Motto: Ich gebe Sicherheit ein Gesicht*

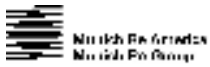
CISO – Chief Information Security Officer  
GISC – Global Infrastructure and Services Committee  
GSCM – Group Security and Continuity Management

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

- Kerngeschäft ist das Management großer und größter Risiken
- Unsere Kunden sind 5.000 Risikoträger weltweit (Versicherer)
- Ca. 7.000 Mitarbeiter (in mehr als 200 verschiedenen Berufen)
- Über 60 Büros weltweit (von 2 bis 3.000 Personen)
- Hauptsitz ist München
- Bruttobeiträge in 2007: 37 Mrd €; Konzernergebnis 3,9 Mrd € Gewinn
- Globales Netzwerk, fortschreitende Standardisierung (z.B. VISTA Client)
- Globale Sicherheitsorganisation (Mandat, Regelwerk, Berichtslinien)
- Ca. 40.000 weitere Mitarbeiter in der Erstversicherung
- 600 Mitarbeiter im Asset Management

## Münchener-Rück-Gruppe

### Rückversicherung



### Erstversicherung

**ERGO**

**DKV**

**VICTORIA**

**HESTIA**

Karstadt Quelle  
Versicherungen



**HAMBURG  
MANNHEIMER**

**ERGO**  
Praxispartner

ERGOISVICRE

**MERCUR ASSISTANCE**  
LES ASSURÉS DE LA SOCIÉTÉ DES ASSURÉS MUNICH RE GROUP

**DIE EUROPÄISCHE**  
Europäische Feuerversicherung AG

Watkins Syndicate

### Assetmanagement

**MEAG**

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

Sicherheit setzt sich aus allen Maßnahmen zusammen, mit denen die Mitarbeiter sowie Sach- und Informationswerte eines Unternehmens präventiv wie reaktiv geschützt werden.

Elektronische Daten  
und Systeme

Papier und  
Räumlichkeiten

Kommunikation und  
Wissen

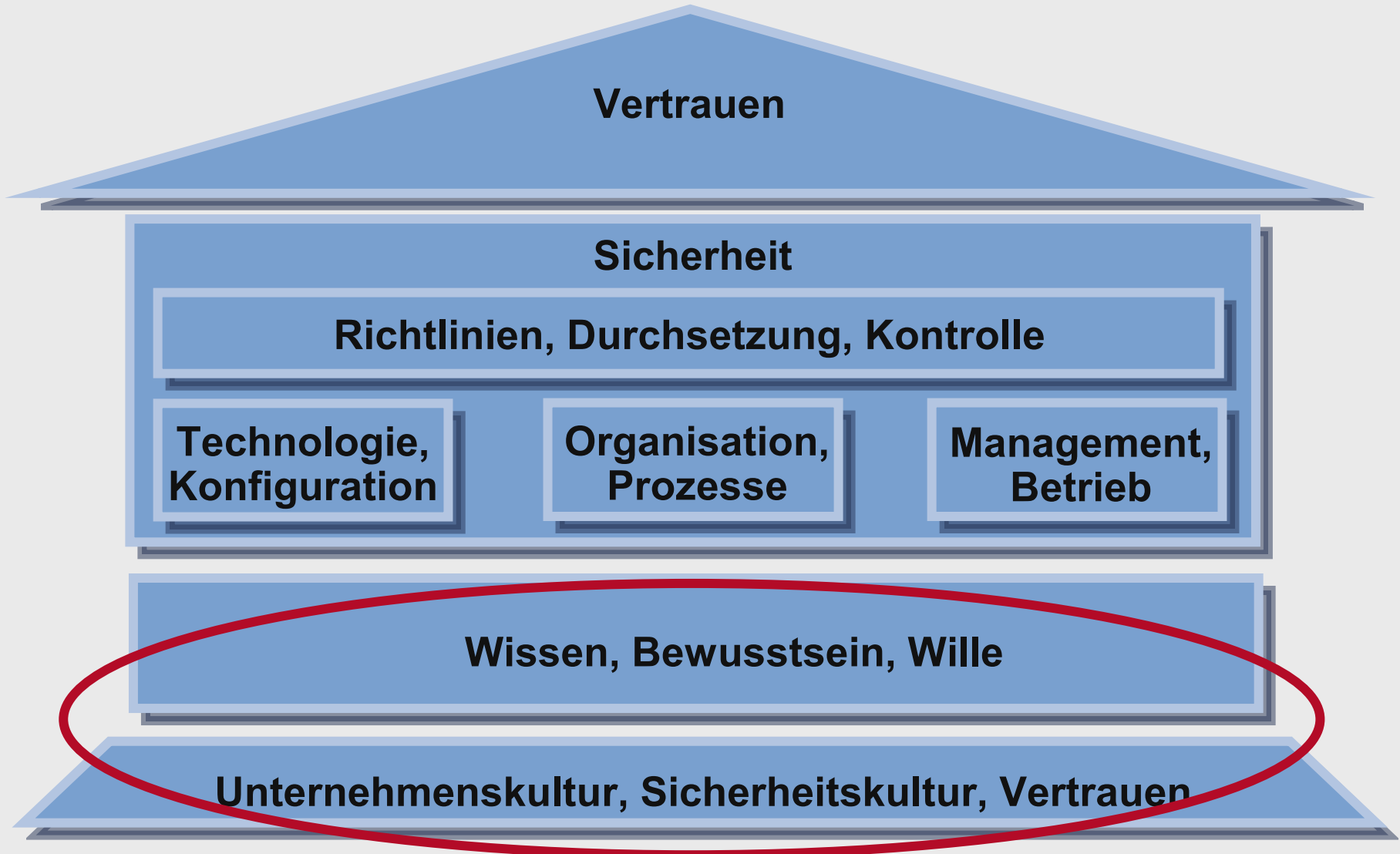
IT-Sicherheit

Bewusstsein,  
Zuverlässigkeit

Informationsschutz

Objektschutz

Personenschutz



## Starke Kettenglieder

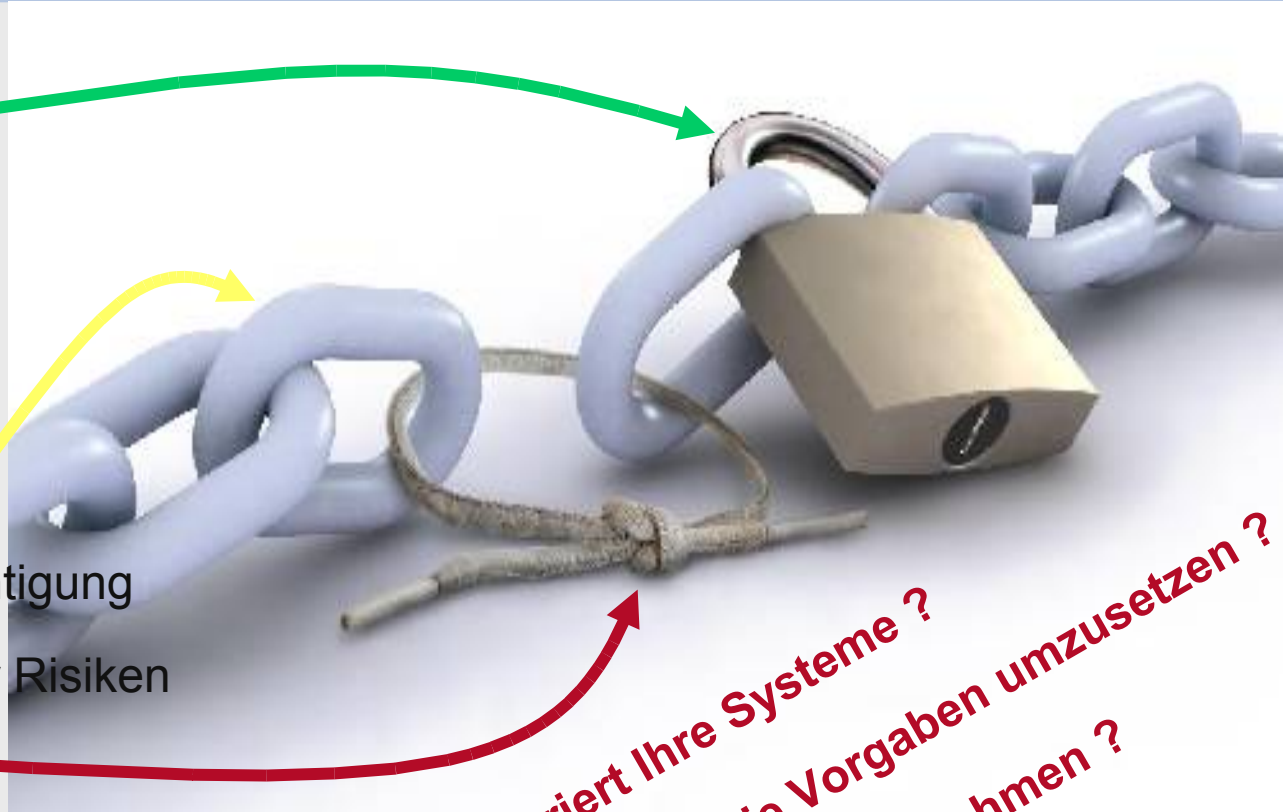
- Firewall
- Virens Scanner
- Schlösser, Schleusen

## Akzeptable Lösungen

- Zugangs-/Zugriffsberechtigung
- Identifizieren potenzieller Risiken

## Schwachpunkte

- Konsistente System Konfiguration
- Durchsetzung der Vorgaben
- Balance zwischen Funktionalität und Sicherheit



*Wer konfiguriert Ihre Systeme ?  
Wer ist beauftragt die Vorgaben umzusetzen ?  
Wer entscheidet über Maßnahmen ?*

**Menschen**

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

- 1987 Einführung erster PCs bei MRM
- 1990 erste Computervirusinfektion
- 1992 erster Virenschutzbeauftragter ernannt
- 1993 erster IT-Sicherheitsbeauftragter ernannt
- 1994 PC-Handbuch für int'l Büros enthält Sicherheitsregeln
- 1998 Sicherheit wird global betrachtet
- 1999 erster CISO für MR Rückversicherungsgruppe ernannt
- 2000 internes Expertenteam für technische Sicherheit aufgebaut
- 2001 Konzernweite Sicherheit auf Arbeitsebene etabliert
- 2003 Security Awareness Programm gestartet
- 2005 Sicherheit sitzt im Infrastruktur-Komitee
- 2008 Ausdehnung des Sicherheitsmandats auf die gesamte MR Gruppe (inkl. BCM) und Ansiedlung im Integriertd Risk Mgmt

0

Bedeutung des Informationsrisiko-Management

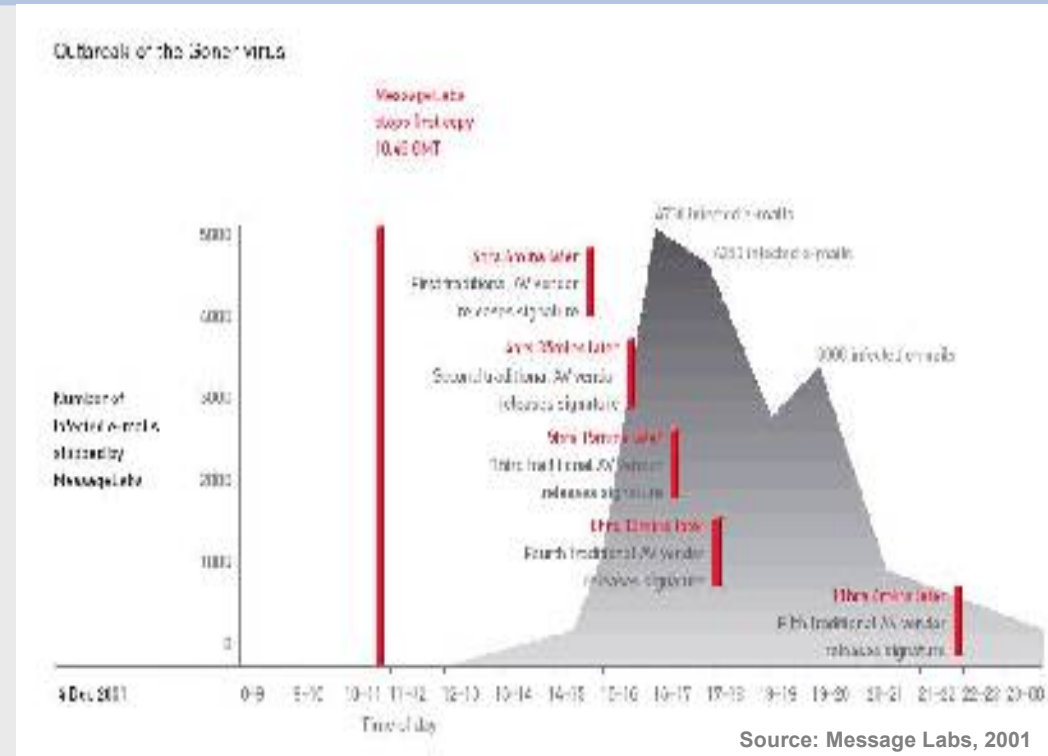
+

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

# Warum wurde das Programm initiiert ?

## Schlechte Erfahrungen

- Das Wesen Mensch
- Prinzip des schwächsten Glieds
- Überzeugung



Interne Ausbreitung erfolgte aufgrund mangelnden Sicherheitsbewusstseins

# Warum wurde des Programm initiiert ?

- Schlechte Erfahrungen

## Das Wesen Mensch

- Prinzip des schwächsten Glieds

- Überzeugung

Gewohnheit

Vergesslichkeit

Risikoeinschätzung

Stress

Wissen

Kultur

Bereitschaft → Motivation → Wille → Verhalten

# Warum wurde das Programm initiiert ?

- Schlechte Erfahrungen
- Das Wesen Mensch

## Prinzip des schwächsten Glieds

- Überzeugung

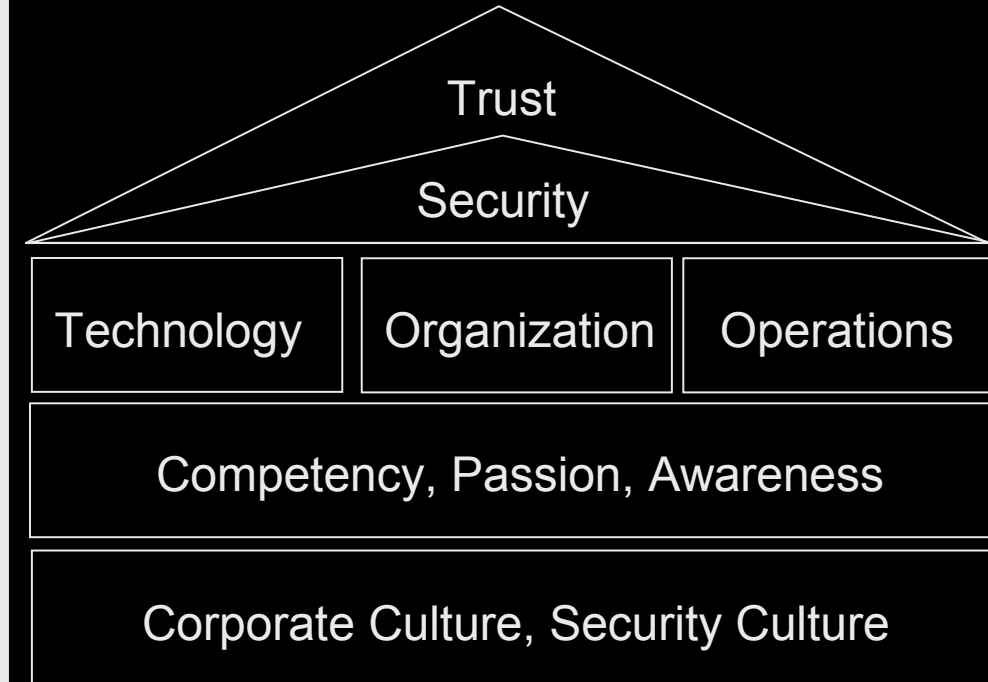


Schwachstellen werden identifiziert und minimiert

# Warum wurde das Programm initiiert ?

- Schlechte Erfahrungen
- Das Wesen Mensch
- Prinzip des schwächsten Glieds

## Überzeugung



Vertrauen baut auf ein  
solides Fundament

- steht im Zentrum des Interesses
- stellt das größte Risiko dar
- stellt die größte Chance dar
- lohnt die Investition



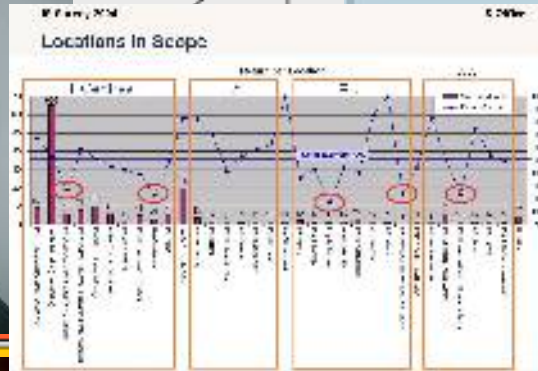
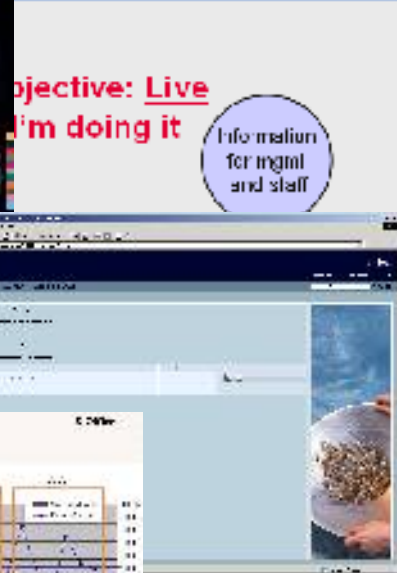
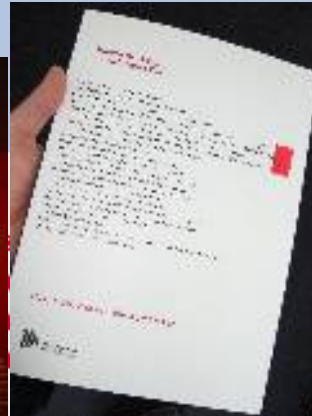
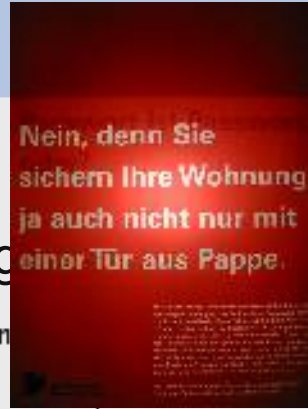
## Maßnahmen erfolgen

- nicht zum Selbstzweck sondern
- zum Schutz des Arbeitsplatzes jedes einzelnen und
- zum Schutz des Unternehmens

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

# Module des Programms

- Sicherheitsmesse
- Webbased Training
- Installationen
- Mitarbeiterforen
- Intranet Website
- Mitarbeitermagazin
- Geschäftsbericht
- Externe Vorträge
- Poster
- Interaktion, . . .



... ist nicht nur ein Training sondern ...

- nutzt verschiedenste Kanäle
- permanente Maßnahme
- interessant und aktuell
- überzeugt statt zu manipulieren
- hilfreich und motivierend
- respektiert unterschiedliche Kulturen
- professionell
- entspricht der Corporate Identity
- reizt zu aktiver Beteiligung
- liefert persönlichen Mehrwert

- Einleitung
- Das Produkt „Sicherheit“
- Geschichte und Organisation
- Die Zielgruppe „Mensch“
- Das Security Awareness Programm
- Schlüsselerlebnis „Social Engineering“

- Verstehen die Mitarbeiter ihre Verantwortung bzgl. Sicherheit ?
- Verstehen sie die Sicherheitsrichtlinien und befolgen sie diese ?
- Wissen sie welche Informationen als vertraulich zu klassifizieren sind ?
- Behandeln sie vertrauliche Informationen entsprechend ?
- Sind sie sich der Angriffe gegen ihre Person bewusst ?
- Berichten sie verdächtige Vorgänge auf angemessene Weise ?

## → Sicherheitsumfrage (Fragebogen)

- Menschen sind zu wenig eingebunden
- Ergebnisse sind nicht objektiv

## → **Social Engineering Assessment**

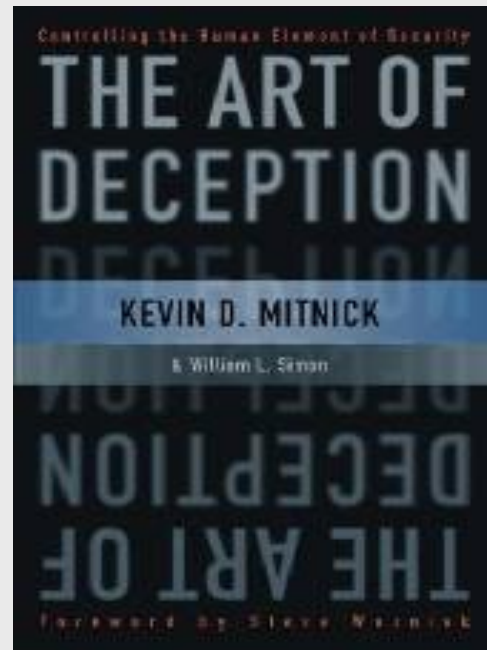
- **Menschen sind aktiv eingebunden**
- **Ergebnisse sind objektiv**
- **Diese Bedrohung kann permanent aufrecht erhalten werden**
- **Erinnert die Menschen an Vorgänge, die sie wirklich erlebt haben**

## → Webbasiertes Training incl. Zertifizierung

... ist eine Form des Informationsdiebstahls durch gezieltes Manipulieren von Menschen, zu denen ein ausschließlich diesem Zweck dienendes Vertrauensverhältnis aufgebaut wurde.



Kevin Mitnick



Michael Rambach

Bei einem Social Engineering **Assessment** werden derartige Mechanismen eingesetzt, um festzustellen ob und mit wie viel Aufwand man an die gewünschten Informationen gelangt.

## Vorbereitung

Definition des Vorgehens

Ziel: Risiko erkennen, Anonymität wahren

## Beschluss

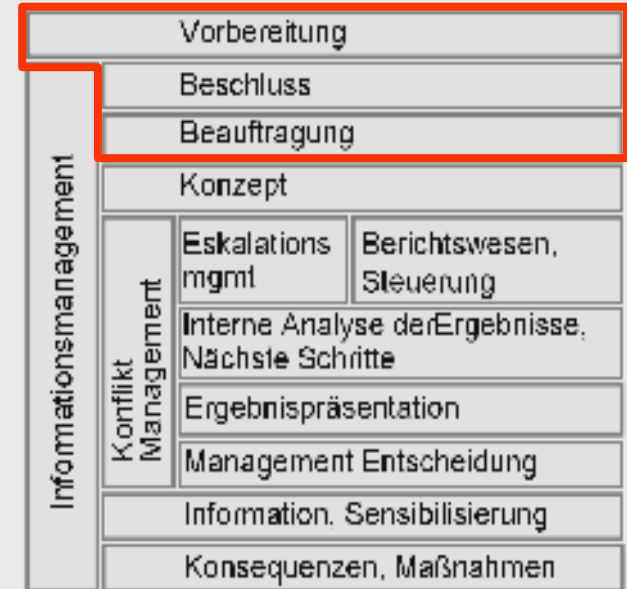
Randbedingungen, Zielobjekte

Budget, Information, Verantwortlichkeiten

## Beauftragung

Externer Auftragnehmer (pros, cons)

Verlässlichkeit, Expertise, Unabhängigkeit



- Sehr kurzfristige Beauftragung
- Sehr enger Zeitrahmen für die Durchführung
- Durchführung während der Urlaubszeit
- Vorgegebene Zielobjekte (Informationen)
- Auftragnehmer hatte weder Rückversicherungs- noch finanzspezifisches Knowhow
- Sehr nah an der Realität:
  - Informierter Personenkreis sehr klein (4 Personen)
  - Vorhandene Schutzmaßnahmen bleiben aktiv
  - Keine Sonderrechte oder Vorabinformationen (= alles selbst erarbeitet)
  - Einschränkungen:
    - Verfügbarkeit des Geschäftsbetriebs nicht beeinträchtigen (so weit möglich)
    - Nichts physisch beschädigen

- Personaldaten
- Finanzdaten
- Personbezogene Versicherungsdaten
- Sitzungsprotokolle
- Reisedaten

## Konzept

3 Phasen Modell

## Berichten und dokumentieren

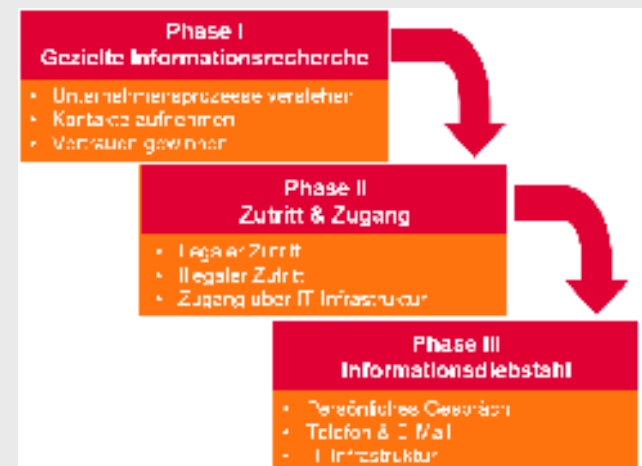
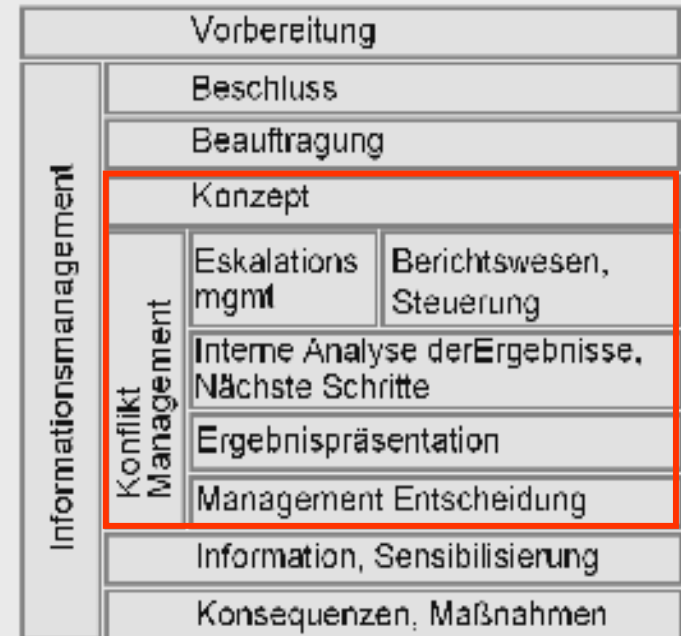
Kickoff (formaler Startpunkt)

Informationskanäle

## Krisenmanagement

Wer ist informiert

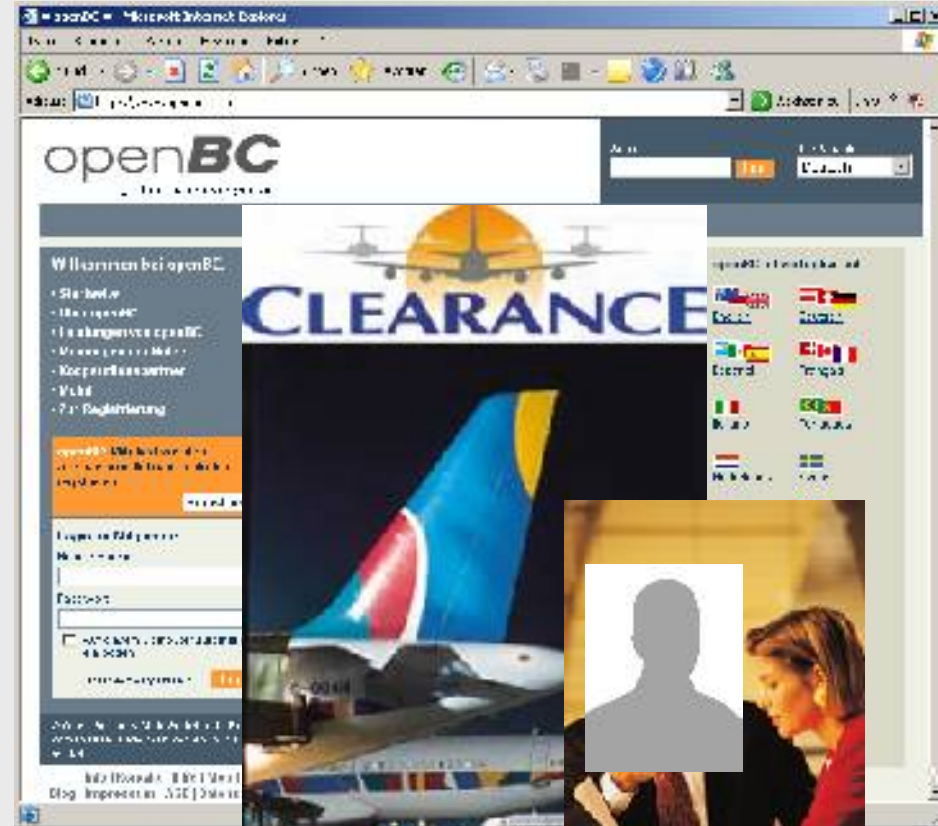
Unmittelbarer Handlungsbedarf



# Phase 1 – Informationsrecherche

## Phase 2 – Zutritt und Zugang

Welches Hacking-Tool ist im Internet für jeden verfügbar ?



# Struktur eines Social Engineering Assessments

## Information, Sensibilisierung

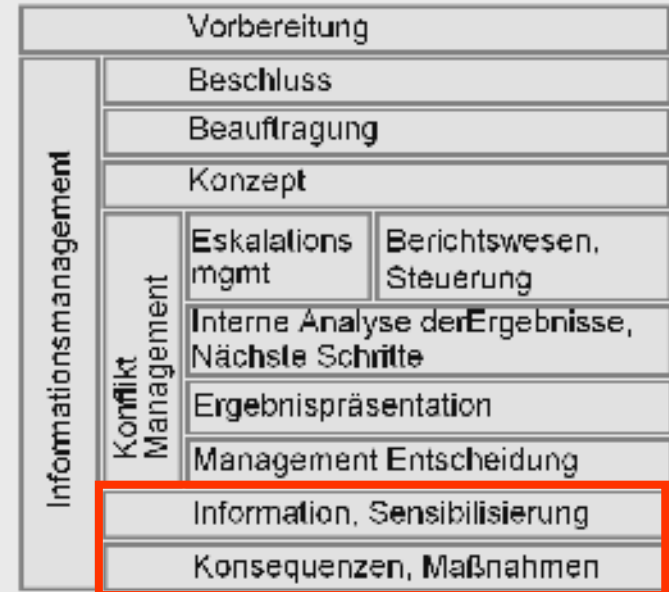
Vorstand

Information der Mitarbeiter

Erkenntnisse für Schulungen nutzen

## Maßnahmen

Follow-up Projekte



- Zugang zu Gebäude und Büros
- Nutzung der technischen Infrastruktur
- Passwörter
- Besprechungen
- Phishing
- Mobile Geräte und Datenträger
- Vertrauliche Papiere
- Abfall

**“Like an egg shell”**

Hard and crunchy on the outside

Soft and chewy on the inside

**Je ausgereifter die technische Sicherheit ist,  
desto einfacher ist Social Engineering!**



- Anzahl der Informierten klein, aber auch groß genug halten
- Einen zuverlässigen, externen Partner beauftragen
- Zeitbegrenzung, Randbedingungen, Zielobjekte vorgeben
- Geeignete Vertraulichkeitserklärung und Vertrag
- Top Management persönlich einbinden
- Folgeaktivitäten unmittelbar starten und durchführen

## Schlüsselerlebnis

- Die Maßnahme war und ist die beste Awareness Maßnahme
- Kontrollierbare Unsicherheit hilft
- Aktive Beteiligung und Erzeugen eines persönlichen Mehrwerts/Reizes

- Wenn Sie . . .
- gut vorbereitet
- zielorientiert
- passioniert
- geduldig
- . . .

. . . vorgehen, arbeiten sie wie ein Social Engineer und erreichen das, was sie erreichen wollen:

- Sie überzeugen ihr Top Management
- Sie initiieren eine Verbesserung der

# Sicherheitskultur



Gibt es etwas besseres, um Sicherheit zu „verkaufen“ ?



Ja

# Einen richtigen Vorfall !

Aber dieser ist bestimmt teurer und riskanter als ein Social Engineering Assessment.



# Danke für Ihre Aufmerksamkeit

Michael Lardschneider, CISO  
Münchener Rück



Münchener Rück  
Munich Re Group



„Rambach“ ist ein Angreifer\*) der

- gut **vorbereitet** ist (vermittelt Kompetenz)
- **zielgerichtet** arbeitet (kein Zufallsangriff)
- **anonym** agiert (verbirgt seine Identität)
- sich **dreist** verhält (Frechheit siegt)
- **selbstbewusst** auftritt (hoher Überzeugungsgrad)
- **flexibel** ist (schauspielerisches Können)
- **psychologische** Fähigkeit hat (Überzeugungskunst, Manipulation)
- meist **unerkannt** bleibt



\*) männlich/weiblich

Measures		preparation	processing	follow up
Posters	2.000 €	content, layout	n/a	n/a
Installations	2.000 €	development	n/a	uninstalling
Flyers	4.000 €	content, approval	n/a	updating
Game	3.000 €	concept, content	performing	awarding
Website	100.000 €	design, promotion	maintenance	updating
Classroom training	40.000 €	concept, content	performing	updating
Webbased training	65.000 €	design, content	maintenance	updating
Staff forums	15.000 €	speakers, agenda	performing	n/a
Security fair (exhibition)	200.000 €	concept, equipm.	performing	uninstalling
Social engineering assessment	22.000 €	concept, contract	observing	projects

# Effektivität (Einfluß auf das Sicherheitsbewusstsein)



Diese Benchmarking-Ergebnisse können nicht ohne weiteres auf andere Unternehmen übertragen werden.

Measures	time/effort	acceptance	awareness effect	measurement
Posters	Low	Fair	Low	# of questions, observe reaction
Installations	Low	Good	High	observe reaction, feedback
Flyers	Low	Fair	Medium	used as reference, # taken
Game	Very low	Very good	Low	# forms, hits at website
Website	High	Low	Low	hits, feedback, critical remarks
Classroom training	Medium	Fair	Medium	bandwidth of participants
Webbased training	High	Low	Medium	# of users
Staff forums	Low	Good	High	# of attendees endurance
Security fair (exhibition)	Very high	Very good	High	# of visitors feedback
Social engineering assessment	Medium	Zero - High	Very high	rumors, mgmt attention

# Effizienz (Verhältnis von Investition und Ergebnis)

Diese Benchmarking-Ergebnisse können nicht ohne weiteres auf andere Unternehmen übertragen werden.

Measures	time/effort	efficiency	awareness effect	measurement
Posters	Low	Fair	Low	cost vs reaction
Installations	Low	Good	High	cost vs reaction
Flyers	Low	Fair	Medium	cost vs usage
Game	Very low	Low	Low	seriousness
Website	High	To low	Low	cost vs usage
Classroom training	Medium	Low	Medium	sustainability
Webbased training	High	To low	Medium	cost vs usage
Staff forums	Low	Very good	High	cost vs publicity
Security fair (exhibition)	Very high	Fair	High	sustainability
Social engineering assesment	Medium	Outstanding	Very high	consternation