TeleTrusT
Pioneers in IT security.

TeleTrusT-Informationstag "Cyber Crime"

Berlin, 20.05.2011

Dr. Christiane Bierekoven
Rödl & Partner, Nürnberg

Rechtliche Aspekte der Wirtschaftsspionage durch Social Engineering

Ihr Ansprechpartner

Dr. Christiane Bierekoven
Associate Partnerin / Rechtsanwältin
Leiterin des IT-Kompetenzcenters

E-Mail: Christiane.Bierekoven@roedl.de

Rödl Rechtsanwaltsgesellschaft
Steuerberatungsgesellschaft mbH
Äußere Sulzbacher Str. 100
90491 Nürnberg
Tel. (0911) 91 93 - 1511
Fax (0911) 91 93 - 1599

Rödl & Partner

Agenda:

1. **Die Bedeutung von Social Networks für Social Engineering**

2. **Bedeutung von Social Networks für das Marketing**

3. **Angriffsszenarien durch Social Engineering**
   a) Vorgehensweise bei Social Engineering
   b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mensch“

4. **Risikopotenziale – Schadensszenarien**
   a) Datenklau
   b) Abgreifen von Know-how
   c) Rufschädigung

Rödl & Partner

Agenda:

5. **Rechtliche Verteidigungsstrategien**
   - a) zivilrechtlich
   - c) arbeitsrechtlich
   - d) strafrechtlich

7. **Restrisiko – Stichwort: repressive Verantwortlichkeit**

9. **Abwehr- und Schutzstrategien – Stichwort: Prävention**
   - a) Ausgangsüberlegung
   - b) Entwicklung von Social Media Strategies
   - c) Key Elements of Social Media Guidelines +

10. **Fazit**

Rödl & Partner

Agenda:

1. **Die Bedeutung von Social Networks für Social Engineering**

2. **Bedeutung von Social Networks für das Marketing**

3. **Angriffsszenarien durch Social Engineering**
   a) Vorgehensweise bei Social Engineering
   b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mesch“

4. **Risikopotenziale – Schadensszenarien**
   a) Datenklau
   b) Abgreifen von Know-how
   c) Rufschädigung

1) Die Bedeutung von Social Networks für Social Engineering

Mark Zuckerberg answering a reporter´s question about why Facebook succeeded:

*„If you give people a better way **to share information** it will change people‘s lives.“* *****

* Quelle: David Kirkpatrick „the facebook effect“, Seite 278,

1) Die Bedeutung von Social Networks für Social Engineering

These:

Social Networks eröffnen Social Engineering neue Möglichkeiten zum

- Datenklau
- Abgreifen von Know-how

Begründung:

- zunehmender Einsatz von Social Networks durch Unternehmen für Marketing und PR
- **Kernelemente** von Social Networks sind:
  - Mitglieder
  - Interaktion / Kommunikation

  = Interaktion / Kommunikation der Mitglieder *„to share information“*

Agenda:

1. Die Bedeutung von Social Networks für Social Engineering
2. **Bedeutung von Social Networks für das Marketing**
3. Angriffsszenarien durch Social Engineering
   a) Vorgehensweise bei Social Engineering
   b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mesch“
4. Risikopotenziale – Schadensszenarien
   a) Datenklau
   b) Abgreifen von Know-how
   c) Rufschädigung

2) Bedeutung von Social Networks für das Marketing

a) Bedeutung für Marketingstrategien

- Verbreitung von Social Media in Deutschland:

  März 2010: ***30 Mio. Deutsche in Internet-Communities****

  davon größte Anzahl in: ***Facebook, VZ-Netzwerken, YouTube, Twitter, Blogs, Xing, Wikipedia****

b) Begründung

- Interaktionsmöglichkeiten mit Kunden

  ⇒ Kundenpflege und –akquisition einschließlich Erschließung neuer Zielgruppen

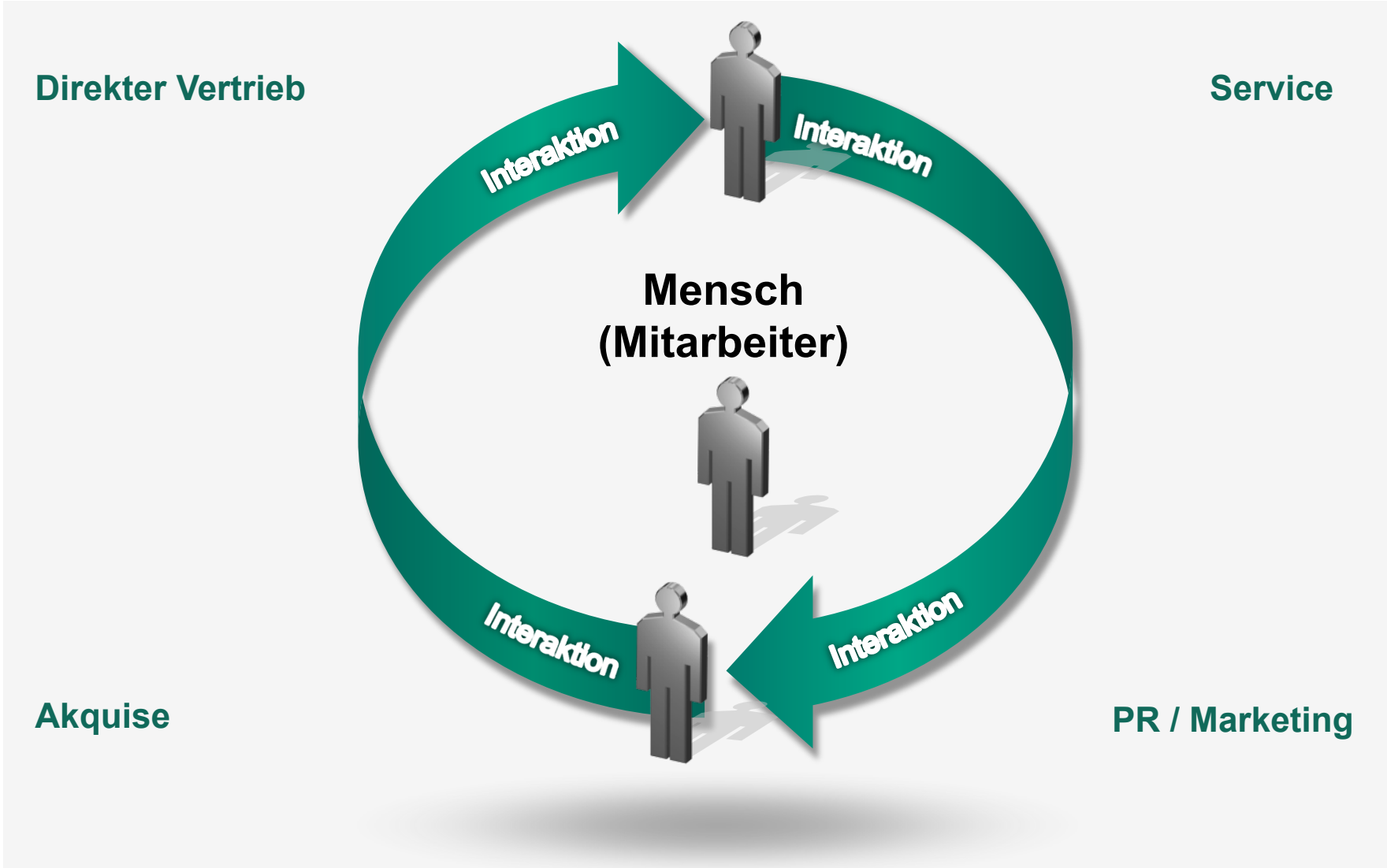
- Verbesserung des Service durch Interaktion über Facebook, Twitter, Blogs

  ⇒ Kundenservice in direkter Interaktion in der Sprache des Kunden

  ⇒ **d.h.**

* Quelle: BITKOM Leitfaden „Social Media“, 2010, S. 4

2) Bedeutung von Social Networks für das Marketing



Rödl & Partner

Agenda:

1. Die Bedeutung von Social Networks für Social Engineering

2. Bedeutung von Social Networks für das Marketing

3. **Angriffsszenarien durch Social Engineering**
   a) Vorgehensweise bei Social Engineering
   b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mesch“

4. Risikopotenziale – Schadensszenarien
   a) Datenklau
   b) Abgreifen von Know-how
   c) Rufschädigung

3) Angriffsszenarien durch Social Engineering

a) Vorgehensweise bei Social Engineering

Kernelement: Ausnutzen menschlicher Eigenschaften, wie Hilfsbereitschaft, **Vertrauen**

Angst / Respekt vor Autorität*

Strategie bei systematischem Social Engineering:

Aufbau einer längeren Beziehung zum Opfer*

b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mensch“

Folge: Bei erfolgreichem Aufbau einer Vertrauensbeziehung:

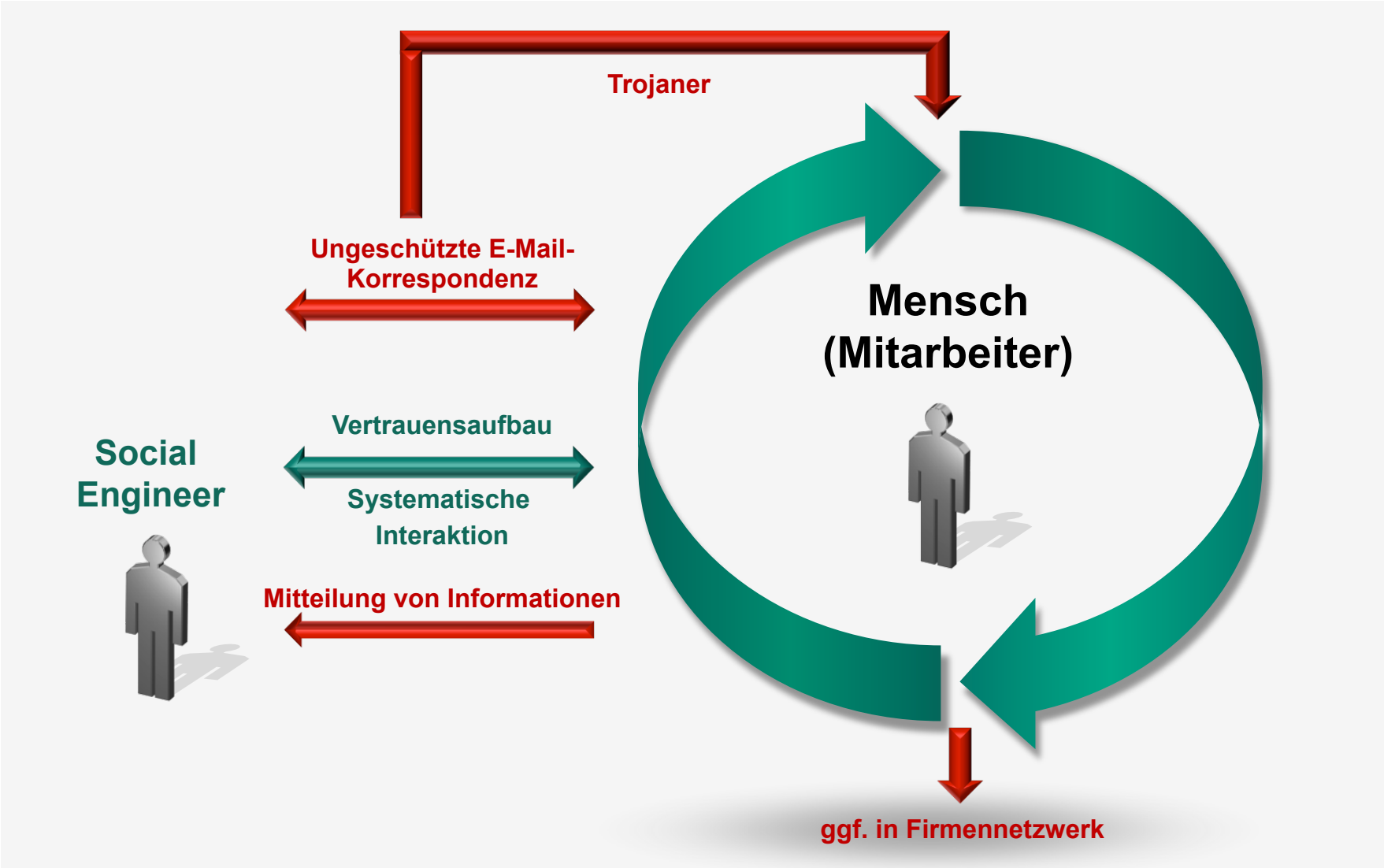
- Abgreifen von Informationen
- Übersendung von Trojanern als E-Mail-Anhang zum Ausspähen weiterer Informationen auf Rechner / Firmen-Netzwerk

d) Erfolgreiches Social Engineering durch Nutzung von Social Networks heißt:

---

* Quelle: IT-Grundschutzkataloge BSI, G 5.42 Social Engineering

3) Angriffsszenarien durch Social Engineering



3) Angriffsszenarien durch Social Engineering

Beispiele:

1. **Datenleck Mitarbeiter – Wirtschaftsspionage via Web 2.0**

   (Quelle: managerSeminare 03.05.2011, 16:01:00 Uhr

   URL: http://www.managerseminare.de/ms_Artikel/Wirtschaftsspionage-via-Web-20-Datenleck-Mitarbeiter,205063)

   „ Mit Robin Sage möchte jeder gerne befreundet sein. Sie sieht auch einfach nett aus: schwarze Haare mit einer blonden Strähne in der Stirn, dunkle Augen, umrandet von einem dicken Kajalstrich. 266 Freunde zählt die junge Dame auf Facebook. Überwiegend Männer, einige davon in verantwortungsvollen Positionen. Manche plaudern mit ihr über Interna von ihrem Arbeitsplatz, besonders Blauäugige schicken ihr sogar – nur um ihr zu gefallen – vertrauliche Dokumente zu und laden sie zu Konferenzen ein. Dorthin kommen kann die Dame allerdings nicht: Sie existiert nicht.“

   (Stichwort: „Die gefakte Mata Hari“)

3) Angriffsszenarien durch Social Engineering

2. Innenministerium warnt vor zunehmender Wirtschaftsspionage

(Quelle:CIO Service-Box, 07.04.2011)

URL: http://www.cio.de/2271009

*„**Angriffe auf das Know-how deutscher Unternehmen** aus dem Internet stellen nach Einschätzung des Bundesministeriums eine **zunehmende Bedrohung** dar.*

…

*Nach Angaben des Ministeriums **verursacht** Wirtschaftsspionage in Deutschland einen **jährlichen Schaden von 20 bis 50 Milliarden EUR.***

…

*Betroffen sei praktisch jedes Unternehmen, unabhängig von seiner Größe. Allerdings gingen **70 Prozent** aller Fälle von Wirtschaftsspionage **auf Mitarbeiter aus** dem **Unternehmen** selbst zurück, aufgrund von Problemen wie Vertrauensschwund oder Arbeitsplatzverlust.“**

---

* Auslassungen von der Verfasserin

3) Angriffsszenarien durch Social Engineering

3. Broschüre „Schrankenlose Offenheit – „soziale Netzwerke“ im Web“

(Quelle: Verfassungsschutz, Stand: August 2010)

„Soziale Netzwerke – ein selbstverständliches Kommunikationsmittel“

…

„Ein Sicherheitsrisiko für das eigene Unternehmen?

Ja, denn viele Nutzer dieser Plattformen offenbaren unbewusst sensible Informationen.“

…

„Mögliche Folgen schrankenloser Offenheit

Angreifer missbrauchen diese Informationen z. B. für:

- *Daten- oder Identitätsdiebstahl*
- *Spam- und Phishing-Attacken*
- *Social Engineering*
- *Illegalen Datenhandel“**

---

* Auslassungen von der Verfasserin

3) Angriffsszenarien durch Social Engineering

4. Broschüre „Sicherheitslücke Mensch – Der Innentäter als größte Bedrohung für die Unternehmen“

(Quelle: Verfassungsschutz, Stand: August 2010)

„Unternehmensspezifisches Know-how entscheidet über Markt- und Zukunftschancen. Spionage, Diebstahl, Sabotage, Korruption oder IT-Kriminalität durch eigene Mitarbeiter bedroht diesen Wettbewerbsvorteil.

….

*Das **Risiko Opfer von Know-how-Abfluss durch Innentäter zu werden,** wird **von** den **meisten Unternehmen** stark **unterschätzt!***

…

30% Außentäter

…

***70% Innentäter“**

* Auslassungen von der Verfasserin

Rödl & Partner

Agenda:

1. Die Bedeutung von Social Networks für Social Engineering

2. Bedeutung von Social Networks für das Marketing

3. Angriffsszenarien durch Social Engineering
   a) Vorgehensweise bei Social Engineering
   b) Kernelement erfolgreichen Social Engineerings: „Risikofaktor Mesch“

4. **Risikopotenziale – Schadensszenarien**
   a) Datenklau
   b) Abgreifen von Know-how
   c) Rufschädigung

4) Risikopotenziale - Schadensszenarien

a) Datenklau

- Durch gezieltes Ausforschen eines Mitarbeiters nach Etablierung von Vertrauen
- Versendung von Trojanern via E-Mails

b) Abgreifen von Know-how

- Durch gezieltes Ausforschen eines Mitarbeiters nach Etablierung von Vertrauen
  - ➢ Beispiel: „Gefakte Mata Hari“ (Folie 13)
- Gezieltes Ausforschen durch Versendung von Trojanern via E-Mail

4) Risikopotenziale - Schadensszenarien

c) Rufschädigung

- Bei Bekanntwerden von Datenlecks
  - Beispiel: Sony
- Kenntnisnahme von (sensiblen) Daten durch Dritte
  - Beispiel: Kontonummern, Kreditkartendaten
- Verbreitung negativer Unternehmensinterna
  - Beispiel: Negativäußerungen über Arbeitgeber-Unternehmen durch Mitarbeiter

Rödl & Partner

Agenda:

5. **Rechtliche Verteidigungsstrategien**
   - a) zivilrechtlich
   - c) arbeitsrechtlich
   - d) strafrechtlich

7. **Restrisiko – Stichwort: repressive Verantwortlichkeit**

9. **Abwehr- und Schutzstrategien – Stichwort: Prävention**
   - a) Ausgangsüberlegung
   - b) Entwicklung von Social Media Strategies
   - c) Key Elements of Social Media Guidelines +

10. **Fazit**

5) Rechtliche Verteidigungsstrategien

a) zivilrechtlich

aa) Unterlassungsansprüche wegen Geheimnisverrat aus

- §§ 17 UWG i.V.m. § 823 Abs. 2, 1004 BGB analog
- § 823 Abs. 1, 826 i.V.m. § 1004 BGB analog
- §§ 3, 4 Nr. 10 und 11 i.V.m. § 8 UWG bei gleichzeitigem Wettbewerbsverstoß

gerichtet auf Unterlassung

- der Weitergabe
- der Verwertung

} **des Geheimnisses und der Nutzung seiner Ergebnisse**

- der gewerbsmäßigen Herstellung / Benutzung von unlauter nachgebauten Maschinen / Werkzeugen / Software pp.

gegen Mitarbeiter und Social Engineer bzw. dessen Auftragsunternehmen

5) Rechtliche Verteidigungsstrategien

Vorteile dieses Vorgehens:

- Kein Verschuldensnachweis erforderlich
- Untersagung in weitem Umfang möglich
- Urteilsveröffentlichung möglich, § 12 Abs. 3 UWG in Zeitschrift, Rundfunk, Tele- und Mediendienst

Nachteile:

- Nachweis des Geheimnisverrats schwierig zu führen
- Darlegung des Geheimnisses in Gerichtsverfahren
- mögliche Rufschädigung, wenn bekannt wird, dass sensible Daten abgezogen werden konnten

5) Rechtliche Verteidigungsstrategien

Daneben: Beseitigungsanspruch auf

- Vernichtung
- Herausgabe zwecks Vernichtung
- Unbrauchbarmachung

→ - der Unterlagen, - Aufzeichnung über Geheimnis

→ - der aufgrund Geheimnisses hergestellten Gegenstände

bb) Schadensersatzansprüche wegen Geheimnisverrat und Betriebsspionage aus

- § 823 Abs. 2 BGB i.V.m. § 17 UWG
- § 826 BGB: sittenwidrige Schädigung
- § 823 Abs. 2 BGB: Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb

5) Rechtliche Verteidigungsstrategien

gerichtet auf

- Geltendmachung konkreten Schadens einschließlich entgangenem Gewinn
- Fiktive Lizenzgebühr
- Herausgabe des Verletzergewinns

→ **Nach Wahl des (verletzten) Unternehmens (Alternativverhältnis)**

gegen

- Mitarbeiter
- Social Engineer → dessen Auftragsunternehmen

5) Rechtliche Verteidigungsstrategien

Problem:

- Verschuldenserfordernis bei Mitarbeiter

  Begründung: Vorsätzliches Handeln ggf. nicht nachweisbar. Es bleibt Fahrlässigkeit

- Schadensberechnung

  Begründung: Nachweis kompliziert

b) arbeitsrechtlich

- Abmahnung mit Vermerk in Personalakte
- Kündigung

  Problem: fristlose Kündigung nur bei Vorliegen eines wichtigen Grundes

  ⇒ Bei Verrat von Geschäfts- und / oder Betriebsgeheimnissen wohl ja

5) Rechtliche Verteidigungsstrategien

- Schadensersatzansprüche

  Problem: Abgestuftes Haftungsregime

  - Keine Haftung bei leichtester Fahrlässigkeit
  - Quotelung bei mittlerer Fahrlässigkeit
  - Volle Haftung bei grober Fahrlässigkeit und Vorsatz

  Folge:

  Mitarbeiter haftet nur bei Vorsatz und grober Fahrlässigkeit voll:

  ➡ *dies muss nachgewiesen* werden, was bei systematischen Social Engineering problematisch sein kann

  ➡ Selbst bei voller Haftung bleibt Bonitätsrisiko

5) Rechtliche Verteidigungsstrategien

c) strafrechtlich

Es kommen folgende Straftatbestände in Betracht:

- §§ 17, 18 UWG: Verrat von Betrieb- und Geschäftsgeheimnissen
- §§ 202a - 205 StGB: Abfangen / Ausspähen von Daten
- §§ 303a – 303b StGB: Datenveränderung / Computersabotage

Zu beachten: Strafantragserfordernis

Frist: § 77b StGB

- 3 Monate

- ab Kenntnis von Tat und Täter

Rödl & Partner

Agenda:

5. Rechtliche Verteidigungsstrategien

a) zivilrechtlich

c) arbeitsrechtlich

d) strafrechtlich

7. Restrisiko – Stichwort: repressive Verantwortlichkeit

9. Abwehr- und Schutzstrategien – Stichwort: Prävention

a) Ausgangsüberlegung

b) Entwicklung von Social Media Strategies

c) Key Elements of Social Media Guidelines +

10. Fazit

6) Restrisiko – Stichwort: repressive Verantwortlichkeit

sämtliche genannten Ansprüche

- wirken repressiv, **d.h.**

  nachdem die Geschäfts- und / oder Betriebsgeheimnisses / Know-how bereits weitergegeben wurden

- verhindern diese Vorgänge / Handlungen nicht

➡ Deshalb sind erforderlich:

Rödl & Partner

Agenda:

5. **Rechtliche Verteidigungsstrategien**
   a) zivilrechtlich
   c) arbeitsrechtlich
   d) strafrechtlich

7. **Restrisiko – Stichwort: repressive Verantwortlichkeit**

9. **Abwehr- und Schutzstrategien – Stichwort: Prävention**
   a) Ausgangsüberlegung
   b) Entwicklung von Social Media Strategies
   c) Key Elements of Social Media Guidelines +

10. **Fazit**

7) Abwehr- und Schutzstrategien – Stichwort Prävention

a) Ausgangsüberlegung:

Ist der Einsatz von Social Networks sinnvoll für das Unternehmen?

Wenn, **ja**

b) Entwicklung von Social Media Strategies

- durch technische Maßnahmen
- Social Media Guidelines +

zur Verhinderung von Social Engineering

d) Key Elements of Social Media Guidelines +

- Klare Verhaltensregelungen in Bezug auf Interaktion mit anderen Mitgliedern
- Verweis auf Verschwiegenheitspflicht bezogen auf Geschäfts- und Betriebsgeheimnisse
- Verweis auf Datenschutz- und wettbewerbsrechtliche Anforderungen

7) Abwehr- und Schutzstrategien – Stichwort Prävention

- Verweis auf zivil-, arbeits- und strafrechtliche Konsequenzen
- Etablierung von Controlling- und / oder Monitoring-Tools - Einwilligungserfordernis zu beachten
- Abschluss – soweit erforderlich – etwaiger Betriebsvereinbarungen
- Überarbeitung etwaiger bestehender Guidelines zum Social Engineering unter Berücksichtigung des Vertrauenselementes

  Beispiel: *Bisher üblicher Hinweis, E-Mail-Anhänge von unbekannten Absendern nicht zu öffnen, läuft bei Social Engineering leer, da der Täter ein vermeintlich vertrauter „Friend“ (Facebook) ist.*

- **„+“**: Regelmäßige Schulungen zur Sensibilisierung der Mitarbeiter

Rödl & Partner

Agenda:

5. **Rechtliche Verteidigungsstrategien**
   - a) zivilrechtlich
   - c) arbeitsrechtlich
   - d) strafrechtlich

7. **Restrisiko – Stichwort: repressive Verantwortlichkeit**

9. **Abwehr- und Schutzstrategien – Stichwort: Prävention**
   - a) Ausgangsüberlegung
   - b) Entwicklung von Social Media Strategies
   - c) Key Elements of Social Media Guidelines +

10. **Fazit**

8) Fazit

a) Zunehmender Einsatz von Social Networks zu Marketing- und PR-Zwecken.

b) Kernelemente von Social Networks sind Mitglieder / Mitarbeiter.

c) Dies begünstigt systematisches Social Engineering.

d) Hiermit steigt das Risiko des Datenklaus und ungefugten Know-how-Abflusses.

e) Repressiv kann hiergegen

- zivilrechtlich
- arbeitsrechtlich
- strafrechtlich

vorgegangen werden.

8) Fazit

f) Es verbleibt das Restrisiko, dass Daten und Know-how weg sind und vom Konkurrenten verwendet worden sein können.

g) Erforderlich sind deswegen präventive Maßnahmen durch

- Technische Schutzvorrichtungen
- Social Media Guidelines +
- Regelmäßige Schulungen der Mitarbeiter

Vielen Dank für Ihre Aufmerksamkeit!

Fragen?
Anmerkungen?