



Bundesamt für  
Verfassungsschutz



Bundesverband

# „Innentäter“ eine unterschätzte Gefahr in Unternehmen

9. Sicherheitstagung des BfV und der ASW  
am 13. Mai 2015 in Berlin



**Deloitte.**

**POWER**  
PERSONEN-OBJEKT-WERKSCHUTZ GMBH

# „Innentäter“ Eine unterschätzte Gefahr in Unternehmen

9. Sicherheitstagung des BfV und der ASW am 13. Mai 2015 in Berlin

Tagungsband

<b>Inhaltsverzeichnis</b>	<b>Seite</b>
<b>Einleitung</b>	<b>1</b>
<b>Grußwort durch den Vorsitzenden der ASW, Volker Wagner</b>	<b>2</b>
<b>– Beitrag des BfV zum Thema: „Innentäter“ – Dr. Hans-Georg Maaßen</b>	<b>6</b>
<b>„Innentäter – eine unterschätzte Gefahr“ Andreas Maack, Chief Security Officer, Merck KGaA</b>	<b>7</b>
<b>„Background Checks – eine effektive Präventivmaßnahme beim Recruiting“ Eckhard Neumann, Geschäftsführer, Signum Consulting GmbH</b>	<b>22</b>
<b>„Identifizierung und Steuerung personeller Risiken mit Business Profiling“ Ralf Kopp, Geschäftsführer, KOPP GmbH</b>	<b>28</b>
<b>„Wirtschaftsschutzgrundhandbuch – Vorhang auf für die ersten Bausteine“ Prof. Timo Kob, Vorstandsmitglied, ASW Bundesverband</b>	<b>54</b>
<b>„Spionage durch Innentäter, so einfach war es noch nie...“ Frank Eckhardt, Leiter Lauschabwehr, Deutsche Telekom AG</b>	<b>63</b>
<b>„Detektion aus der Praxis – Beispiele national / international agierender Unternehmen“ Sandra Wippermann, Gesellschafterin, Detektei – Holler GmbH</b>	<b>67</b>
<b>Bildmaterial</b>	<b>70</b>

„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN

## 9. Sicherheitstagung des BfV und der ASW am 13. Mai 2015 in Berlin



BfV-Präsident Dr. Hans-Georg Maaßen und der ASW-Vorsitzende Volker Wagner

Am 13. Mai 2015 fand die zur guten Tradition gewordene Jahrestagung von BfV und ASW bereits zum neunten Mal statt. Neu war in diesem Jahr, dass erstmalig mit einem Leitmotiv: „Innentäter – eine unterschätzte Gefahr für Unternehmen“ eingeladen wurde. Zu diesem Themenschwerpunkt tauschten sich rund 130 Sicherheitsexperten und Interessierte unter anderem von Sicherheitsbehörden, Unternehmen, Verbänden und Einrichtungen von Forschung und Wissenschaft aus. Daneben bot die Tagung, mit einem erstmals durchgeführten informellen Vorabendtreffen, vielfältige Möglichkeiten zum Kennenlernen und Vertiefen bestehender Kontakte.

Die 10. Sicherheitstagung findet am 9. Juni 2016 in Berlin statt.

## Begrüßung und Eröffnung durch den Vorsitzenden der ASW,

Volker Wagner

Sehr geehrter Herr Präsident, lieber Herr Dr. Maaßen, Liebe ASW Mitglieder, Vertreter der Wirtschaft und der Sicherheitsbehörden, verehrte Gäste: Ich freue mich Sie heute hier auf unserer 9ten BfV/ASW Tagung zum Thema „Innentäter – Eine unterschätzte Gefahr in Unternehmen“ begrüßen zu dürfen.

Wer sich mit dem Thema befasst, wird schnell erkennen, dass Geheimnisverrat durch Innentäter schon so alt ist wie die Menschheitsgeschichte, und in Teilen diese Geschichte auch durch ihre Handlungen verändert wurde. Wer denkt bei Verrat nicht an:

- Judas – Verriet Jesus an die Römer
- Brutus – Verräter und Mitmörder Caesars
- Hagen von Tronje – Verriet und tötete Siegfried in der Nibelungensage
- Fredo Corleone – Verriet seinen Bruder in „Der Pate“
- Günter Guillaume – Verriet Kanzler Willy Brandt an die DDR
- Julius und Ethel Greenglass Rosenberg – Übermittelten Nukleargeheimnisse an die Sowjetunion

Die niederländische Tänzerin Mata Hari wurde von den Deutschen als Spionin bezahlt und dafür 1917 hingerichtet. Wie sich später herausstellte, hatte sie den Deutschen aber keine wichtigen Geheimnisse geliefert.

Doch was bedeutet das für die Wirtschaft? Hier geht es um Begriffe, wie Betriebsspionage, Industriespionage, Werksspionage, Konkurrenzausspähung sowie Know-how-Diebstahl.

Experten sehen für eine konkrete Handlung das Zusammenwirken von den sogenannten „3 Ms“ als entscheidend an.

### 1. Motiv:

Dabei geht es natürlich in erster Linie um finanzielle Motive.

### 2. Moral:

Frustration nach Umstrukturierungen oder Übergehen bei Beförderungen reduzieren die Bindung an das Unternehmen.

### 3. Möglichkeit:

Gerade in diesem Zusammenhang haben Innentäter besondere Möglichkeiten, Kenntnisse, Netzwerke und Werkzeuge. Dies gilt sowohl für eigene Mitarbeiter als auch für Subunternehmer und Berater. Das steigende Gefährdungspotential entsteht durch folgende Faktoren:

**Erstens** ist es für Unternehmen schwer, bei den Mitarbeitern für dauerhafte Awareness zu sorgen.

**Zweitens** ist die moderne mobile Arbeitswelt von der Volatilität der Beschäftigungsverhältnisse geprägt.

**Drittens** erleichtern moderne Kommunikationsformen in sozialen Netzwerken den Informationsabfluss.

Eine Studie der Personalberatung Hays unterstreicht dies anhand konkreter Zahlen. Der Anteil der an externe Büros ausgelagerter Ingenieurleistungen deutscher Unternehmen liegt bei 58 %.

Wenn wir schon bei Zahlen und Studien sind, die Wirtschaftsprüfungsgesellschaft KPMG geht bei den identifizierten Fällen bei jedem zweiten Fall von einem Innentäter aus.

Generell sind die gesetzlichen Vorschriften zum Geheimnisverrat im Strafgesetzbuch und im UWG, dem Gesetz gegen unlauteren Wettbewerb, geregelt. Wegen ihrer besonderen Kenntnisse und Möglichkeiten gibt es darüber hinaus noch besonders zur Geheimhaltung verpflichtete Personengruppen. Als Beispiele möchte ich hier Vorstände, Aufsichtsräte sowie Betriebsverfassungsorgane nennen. Die Regelungen dazu finden sich im GmbH-Gesetz, Aktiengesetz und Betriebsverfassungsgesetz.

Dabei sind die zunehmenden Risiken, insbesondere durch Wirtschaftskriminalität und Wirtschafts- bzw. Industriespionage, deutlich spürbar und fordern Politik, Wirtschaft und Gesellschaft in immer stärkerem Maße zum Handeln auf.

Die Bestrebungen der Politik zu unterstützen und zu fördern, sehe ich als ganz klare Aufgabe der ASW. Als Verband möchten wir einen wertvollen Beitrag leisten indem wir uns

1. als aktiver Partner in der politischen Gesetzgebung positionieren,
2. als Sprachrohr zu den Medien fungieren und
3. unsere Scharnierfunktion zwischen den Sicherheitsbehörden und der Wirtschaft weiterhin stärken.

Dass sich dies am besten mit der geballten Expertenkompetenz unserer Mitglieder bewerkstelligen lässt, zeigen die Ergebnisse aus unseren Kompetenzcentern. Hier haben wir alle wichtigen Sicherheitsthemen in der Bearbeitung und natürlich sind Informationsschutz und Spionageabwehr ein Schwerpunkt.

Ich kann es nicht oft genug betonen: Es ist wichtig, den Wirtschaftsschutz gemeinsam mit den Unternehmen, Sicherheitsbehörden und Verbänden voranzutreiben.

1. Hier sind in erster Linie unsere Partnerschaften mit den Sicherheitsbehörden zu nennen. Da dies bereits die 9te Tagung mit dem BfV ist, können wir hier ja schon von einer Tradition sprechen.
2. Sensibilisierung/ Prävention: Sensibilisierung von Wirtschaft und Behörden für Risiken und Belange des Wirtschaftsschutzes. Hierzu haben wir mit der Firma EXPLOQII einen neuen Film produziert, den wir Ihnen an dieser Stelle kurz vorstellen wollen. – FILM AB! –

Nun aber zum heutigen Tag! Dass Sie so zahlreich erschienen sind, zeigt mir, dass wir hier das richtige Thema ansprechen und es freut mich, Ihnen auch dieses Jahr eine abwechslungsreiche Agenda mit hervorragenden Referenten präsentieren zu können. Das Leitthema unserer heutigen Agenda ist: Innentäter, die unterschätzte Gefahr. Und damit starten wir gleich mit einer sicherlich bereichernden Keynote unseres BfV Präsidenten zur aktuellen Situation. Im Anschluss hören wir einen Praxisbericht aus der Pharmabranche sowie die Darstellung geeigneter Präventionsmethoden bei der Auswahl neuer Mitarbeiter und Geschäftspartner.

Am Nachmittag warten dann auf uns noch weitere praxisorientierte Themen, u. a. zu Ermittlungen und technischer Lauschabwehr.

Zum Abschluss werfen wir noch einen Blick auf den internationalen Terrorismus und dessen Relevanz für deutsche Unternehmen.

Ich bin sicher, auch in diesem Jahr wird unsere „traditionelle“ und bereits 9te BfV/ASW Kooperationsveranstaltung erfolgreich sein. Die langjährige, gute und vertrauensvolle Zusammenarbeit ist die beste Basis für ein gutes Gelingen.

Erlauben Sie mir noch kurz zu erwähnen, eine solche Veranstaltung ist nur mit Unterstützung möglich. Neben dem BfV, mit dem wir als ASW die Organisation und Inhalt des heutigen Tages gemeinsam gestaltet haben, möchte ich mich auch bei unseren Sponsoren Deloitte, der Power Unternehmensgruppe und der Deutschen Telekom bedanken, die mit dazu beigetragen haben, das heutige Setting in diesem Umfang möglich zu machen.



Übrigens haben wir Presse- und Medienvertreter für den ersten Teil der Veranstaltung eingeladen. Und in der Mittagspause findet eine Pressekonferenz statt.

Lassen Sie uns nun mit der Keynote den Tag beginnen: Herr Dr. Maaßen, vielen Dank, dass Sie sich die Zeit genommen haben, um heute hier zu sein und uns in das Thema einzuleiten. Ich weiß, dass Sie sich persönlich des Themas annehmen und uns heute tatkräftig unterstützen. In diesem Sinne, lieber Herr Dr. Maaßen, die Bühne gehört Ihnen!

## – Beitrag des BfV zum Thema: „Innentäter“ –

Dr. Hans-Georg Maaßen

BfV-Präsident Dr. Maaßen erklärte, Menschen stellen eine mögliche Sicherheitslücke dar, die von Unternehmen oft unterschätzt wird. Ein Spionageangriff ist häufig eine Kombination aus elektronischem Angriff und menschlichem Handeln. Unternehmen wie auch Behörden benötigen motivierte und sensibilisierte Mitarbeiter als eine „human firewall“ zum Schutz von illegalem Technologietransfer.

Die erst kürzlich veröffentlichte Sicherheitsumfrage „WIK/ASW Sicherheits-Enquete 2014/2015“ bestätigte diese Einschätzung und erbrachte u.a. das Ergebnis, dass etwa 30% der in den vergangenen zwei Jahren von Unternehmen angezeigten Delikte auf Taten von Mitarbeitern zurückzuführen waren.

Dabei sind „Innentäter“ der Faktor mit dem höchsten Risikopotenzial für Unternehmen. Sie verfügen in der Regel über volle physische und virtuelle Zugangsmöglichkeiten zu Räumlichkeiten, Netzwerken und Datenbanken im Unternehmen und sind zugleich mit den notwendigen sozialen Kontaktmöglichkeiten ausgestattet. Für „Innentäter“ ist es einfach, ergänzende Erläuterungen oder Verfahrensdokumentationen zu erhalten, insgesamt also ein Schadensszenario, das weit über einen elektronischen Angriff hinausgehen, ihn zumindest hervorragend ergänzen kann. Sorglosigkeit im Umgang mit sensiblen Unterlagen einerseits und die vermeintliche Vertrauenssituation zum unerkannten „Innentäter“ andererseits erleichtern die dolosen Handlungen enorm.

Täter kann jeder vom Hausmeister bis zum Manager sein – Hierarchien bilden hierbei keine Grenzen. Als Akteure kommen sowohl langjährig beschäftigte Mitarbeiter in Betracht als auch eingeschleuste oder nur kurzfristig im Unternehmen beschäftigte Personen sowie Fremdpersonal.

Ihre Motivation kann ebenso vielfältig sein. Im Laufe eines Berufslebens erlebte Enttäuschungen – z.B. wegen nicht erfüllter Beförderungswünsche – können den ehemals motivierten zu einem frustrierten Mitarbeiter verändern. Bindung und Solidarität zum Unternehmen („Corporate Identity“) hat er längst verloren, innerlich vielleicht längst gekündigt.


Aber auch vorübergehend im Unternehmen tätiges Fremdpersonal, das zeitlich befristet Zutritts- und Zugriffsberechtigungen erhält, stellt ein Schadensrisiko dar, insbesondere wenn es mit einer bestimmten Auftragsituation eingeschleust wurde oder mit persönlich motivierter Schadensabsicht eindringt.

## „Innentäter – eine unterschätzte Gefahr“




Andreas Maack, Chief Security Officer, Merck KGaA



„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN



## Was wir tun

Healthcare	Life Science	Performance Materials
		
<b>Merck Serono, Consumer Health, Allergopharma, Biosimilars</b>	<b>Merck Millipore</b>	<b>Performance Materials</b>
<p>Verschreibungspflichtige <b>Medikamente</b>, etwa gegen Krebs, Unfruchtbarkeit oder Multiple Sklerose, <b>rezeptfreie Produkte</b> bei Erkältung und Schmerzen, sowie Innovationen im Bereich <b>Allergien</b> und <b>Biosimilars</b>.</p>	<p>Innovative Instrumente und <b>Labormaterialien</b> für die Life-Science-Industrie, die <b>Forschung</b> und <b>Biotech-Produktion</b> einfacher, schneller und erfolgreicher machen.</p>	<p>Spezialchemikalien für besondere Ansprüche wie <b>Flüssigkristalle</b> für Displays, <b>Effektpigmente</b> für Lacke und Kosmetik oder <b>Hightech-Materialien</b> für die Elektronik-Industrie.</p>

9. Sicherheitsstrategie BRV & ASW | 13. Mai 2015



**Healthcare, Life Science & Performance Materials**

1668 gegründet

66 Länder

39.000 Mitarbeiter

1,7 Mrd € für Forschung und Entwicklung 2014

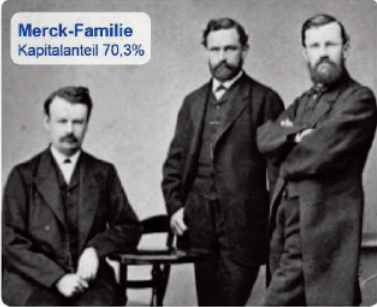
11,3 Mrd € Umsatzerlöse 2014



## Wir sind im Familieneigentum UND börsennotiert

**Merck KGaA**  
Gesamtkapital 100,0%

**Merck-Familie**  
Kapitalanteil 70,3%




Im Familieneigentum seit 12 Generationen

**Aktionäre**  
Grundkapital 29,7%




Börsennotiert seit 1995 - Im DAX seit 2005

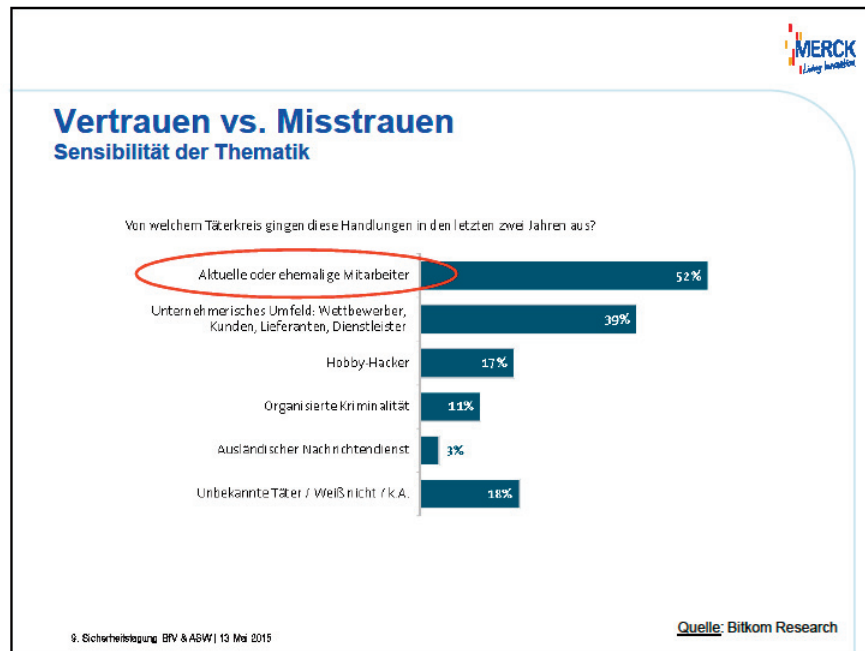
9. Sicherheitskongress BRV & ASW | 13. Mai 2015




## Security Risiken für die Industrie Ein Querschnitt?




9. Sicherheitskongress BRV & ASW | 13. Mai 2015





## Das 'Compliance Komitee'

Beispiel für einen internen Kooperationsmechanismus



9. Sicherheitsagung BRV & ASW | 13 Mai 2015



## Leitgedanken „Innentäter“

Vertrauen vs. Misstrauen

**Kein Generalverdacht**

- Mitarbeiter werden nicht per se verdächtigt und überprüft
- Vertrauen bleibt die Grundlage der Zusammenarbeit
- Agieren der Konzernsicherheit und Schnittstellenfunktionen nach der Unschuldsvermutung

**Risikobasierter Ansatz von Maßnahmen**

- Präventive Maßnahmen richten sich nach dem Betätigungsfeld und daraus resultierenden Berechtigungen.
- Notwendigkeit und Grad von Maßnahmen folgen einer vorangehenden Risikoanalyse / begründeten Verdachtsmomenten
- Orientierung an Tatgelegenheitsstruktur

**Strikte Einhaltung des rechtlichen Rahmens**

- Der rechtliche Rahmen der betreffenden Länder und Deutschlands muss stets eingehalten werden
- Die Gerichtsverwertbarkeit möglicher Ergebnisse ist essentiell
- Berücksichtigung von Mitbestimmungspflichten und Grundlagen der „Gewaltenteilung“

**Transparente Prozesse**

- Kooperation mit Betriebsrat und Sprecherausschuss
- Extern: Sicherstellung der Compliance eines eventuellen Dienstleisters
- Genehmigungsverfahren für bestimmte Maßnahmen über „Compliance Committee“ bzw. Rechtsabteilung

**Kontrolle bleibt stets intern**

- Bei Auslagerungen von Maßnahmen verbleibt die Federführung intern
- Überprüfung und Aufarbeitung der Ergebnisse erfolgt stets durch die Konzernsicherheit
- Etablierung von wirkungsvollen Verteidigungslinien

9. Sicherheitsagung BRV & ASW | 13 Mai 2015

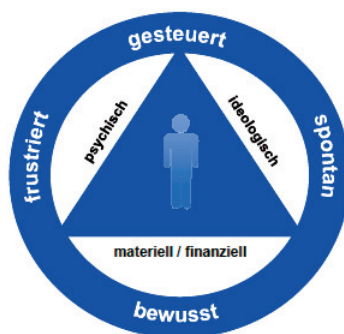
## Deutsche (Chemie-) Industrie im Fokus? Objektive und subjektive Gefährdungskriterien



- ▶ Hohe Know-how Dichte
- ▶ Weltweit anerkanntes („benedetetes“) Industrieland
- ▶ Sicherheit bei vielen Firmen noch immer zu wenig gelebt („Bei uns ist noch nie was passiert!“)
- ▶ Dual-use Produkte haben gefährliches Potential
- ▶ Steigende Bedrohung durch radikale Einzeltäter; inkl. spontaner Selbstradikalisierung
- ▶ Steigende Vernetzung (Globalisierung / Industrie 4.0 / Human 2.0 / ...)

9. Sicherheitsabteilung BRV & ASW | 13. Mai 2015


## Tätertypen und Motive [Entwurf] Erklärungsversuche Tathandeln




- Politische / Ideologische Botschaft
- Anschlag
- Suchtverhalten
- Industriespionage
- Selbstverwirklichung
- Rache
- Wettbewerbsverzerrung
- Suizid
- Sabotage
- Bereicherung
- Aufmerksamkeit
- „Job-hopping“
- Leakage („Wiki-Leaks“)
- ...


9. Sicherheitsabteilung BRV & ASW | 13. Mai 2015











**Konzernsicherheit**  
**Sicherheitslagebild Merck Gruppe 2014 [Auszug]**



9. Sicherheitslagung BVV & ASIW | 13 Mai 2015



**Fallbeispiel 1**  
**Verrat von Betriebsgeheimnissen (Spionage)**

- MA hatte während seiner Arbeitszeit rechtmäßig Zugriff auf sensible und vertrauliche Informationen, die Geschäftsgeheimnisse von Merck begründen.
- Eingang von Hinweisen auf „Vertrauensbruch“ bei Management & Konzernsicherheit
- Nach begründeten Verdachtsmomenten wurde der Laptop des MA eingezogen und forensisch analysiert.
- MA hatte 
- 
- Die Dokumente waren als vertraulich gekennzeichnet und somit für den MA erkennbar, der Mitarbeiter war zudem hinreichend trainiert und sensibilisiert
- Das Arbeitsverhältnis mit dem MA wurde beendet.
- 

9. Sicherheitslagung BVV & ASIW | 13 Mai 2015

 MERCK  
Lebendiger Fortschritt

## Fallbeispiel Datendiebstahl

Rechtslage 



9. Sicherheitslegung BRV & ASW | 13. Mai 2015

 MERCK  
Lebendiger Fortschritt

## Kriterien eines Geschäftsgeheimnisses

### Am Beispiel Deutschland

**(BGH, Urt. v. 27. 04. 2006. I ZR 126/03, Tz. 19 - Kundendatenprogramm)**

*Ein Geschäftsgeheimnis braucht keinen bestimmten Vermögenswert zu besitzen; es reicht aus, dass es sich für den Geschäftsinhaber nachteilig auswirken kann, wenn Dritte, insbesondere Wettbewerber, Kenntnis von den Daten erlangen.*

*Dabei darf es sich nicht lediglich um Angaben handeln, die jederzeit ohne großen Aufwand aus allgemein zugänglichen Quellen erstellt werden können.*

*Ein Geschäfts- oder Betriebsgeheimnis i.S. von § 17 UWG ist jede im Zusammenhang mit einem Betrieb stehende Tatsache, die nicht offenkundig, sondern nur einem eng begrenzten Personenkreis bekannt ist und nach dem bekundeten, auf wirtschaftlichen Interessen beruhenden Willen des Betriebsinhabers geheim gehalten werden soll.*

Betriebsbezogenheit /  
Nichtoffenkundigkeit

Geheimhaltungswille / -Interesse

Kommerzielle Aspekte

maßgebliche Kriterien eines  
Geschäftsgeheimnisses

9. Sicherheitslegung BRV & ASW | 13. Mai 2015



## Fallbeispiel 2

### Unbefugter Zugriff auf Daten

- Externer MA hat berechtigten Zugriff auf sensible Datenbanken
- MA nutzt diese Berechtigung für unautorisierte Änderungen seiner Zugriffsrechte, um sich auch nach Ende des Auftrags weiter Zugriff zu sichern
- Unautorisierte Zugriffe wurden durch Monitoring entdeckt
- MA wollte [REDACTED]
- Gerichtsfeste Aufklärung erfolgte mit Hilfe forensischer Tools
- Strafanzeige wurde durch Merck gestellt
- Einstellung des Verfahrens durch die zuständige StA

9. Sicherheitstagung BRV & ASiW | 13. Mai 2015



## Fallbeispiel 2



- Sichtweise der Staatsanwaltschaft problematisch für das geschädigte Unternehmen
- §202a StGB (Ausspähen von Daten) könnte Lücken im Schutz betroffener Unternehmen aufweisen
- Problemstellung: Nutzung von berechtigten Zugangsdaten für kriminelle / schädigende Handlungen
- Innentäter sind somit nur schwer zu belangen, wenn sie Zugangsdaten zur Ausführung von Aufträgen bekommen und nicht im Wirkbereich von §17 UWG agiert wird

9. Sicherheitstagung BRV & ASiW | 13. Mai 2015

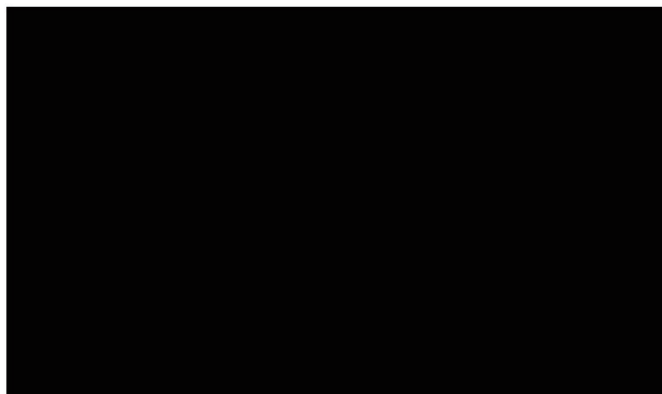
### Fallbeispiel 3 Medikamentendiebstahl

- MA hat berechtigten Zugang zu Warenlager
- MA nutzt diesen zur Begehung von Eigentumsdelikten (Diebstahl / Unterschlagung)
- Missbrauch der „Notfallprozeduren“
- Versagen der Kontrollsysteme
- Ermittlungen der lokalen Polizei
- Qualitätsaspekte für die verbliebene Rest-Charge



9. Sicherheitslegung BRV & ASW | 13. Mai 2015

### Corporate Security




9. Sicherheitslegung BRV & ASW | 13. Mai 2015

MERCK  
Living Innovation

## ‘Dual-use’ Chemikalien

### Proaktive Abzweigungsverhinderung



9. Sicherheitsagung BVV & ASW | 13 Mai 2015 Bildquelle: UNODC

MERCK  
Living Innovation

## Schutz der Kronjuwelen

### Eine gewaltige Herausforderung

# SCHUTZ DER „KRONJUWELEN“

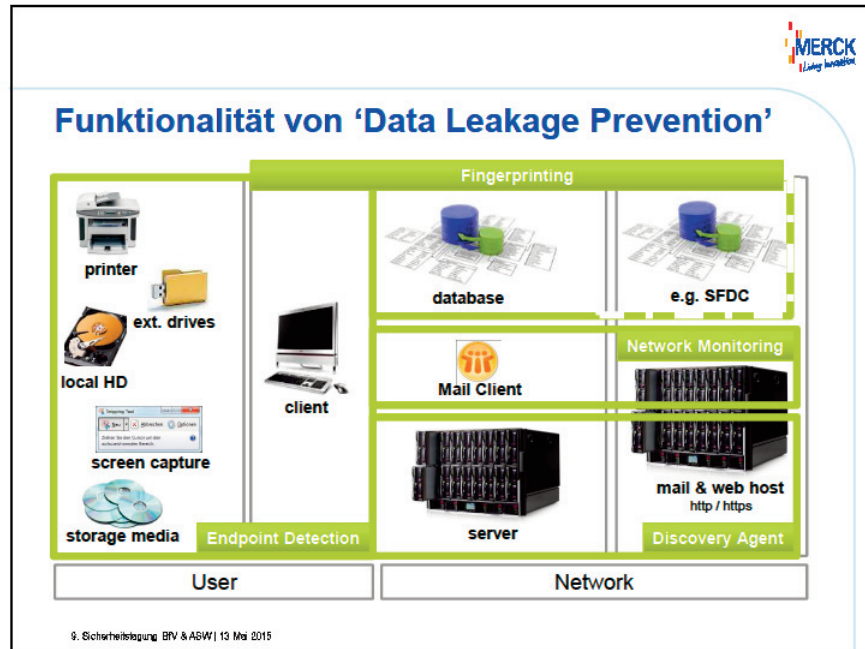
**DATA LEAKAGE PREVENTION** Ein Computerprogramm bei Liquid Crystals sichert wertvolle Merck-Daten vor Verlust – Kampf den Datendieben – Eine wahre Begebenheit



PURES GOLD FÜR WETTBEWERBER

Quelle: Merck Mitarbeiter-Zeitung PRO, April 2014  
Namen von der Redaktion geändert

9. Sicherheitsagung BVV & ASW | 13 Mai 2015





## Präventionsmöglichkeiten

### Notwendigkeit eines ganzheitlichen Ansatzes

	<b>PERSONELL</b>	<ul style="list-style-type: none"> <li>• "need-to-know" Prinzip / Segregieren von Aufgaben</li> <li>• Awareness-Trainings für betreffende MA</li> </ul>
	<b>TECHNISCH</b>	<ul style="list-style-type: none"> <li>• Technische Barrieren aufbauen (physisch / systemisch)</li> <li>• Detektionsmöglichkeiten erhöhen</li> </ul>
	<b>Prozessual</b>	<ul style="list-style-type: none"> <li>• HR: z. Bsp. Abgleich mit Sanktionslisten</li> <li>• Security: u.a. "Pre-employment checks", Access-Management</li> <li>• IT: individualisierte Vergabe von Zugriffsrechten</li> </ul>
	<b>INTELLIGENCE</b>	<ul style="list-style-type: none"> <li>• Diskreter / offener Austausch über Partnerships</li> <li>• „Open-source“- Analysen</li> <li>• Aggregieren von Informationen durch Verbände und Behörden</li> </ul>

9. Sicherheitsagung BRV & ASW | 13 Mai 2015



## Verantwortung für Mitarbeiter

### Innentäter = Mitarbeiter

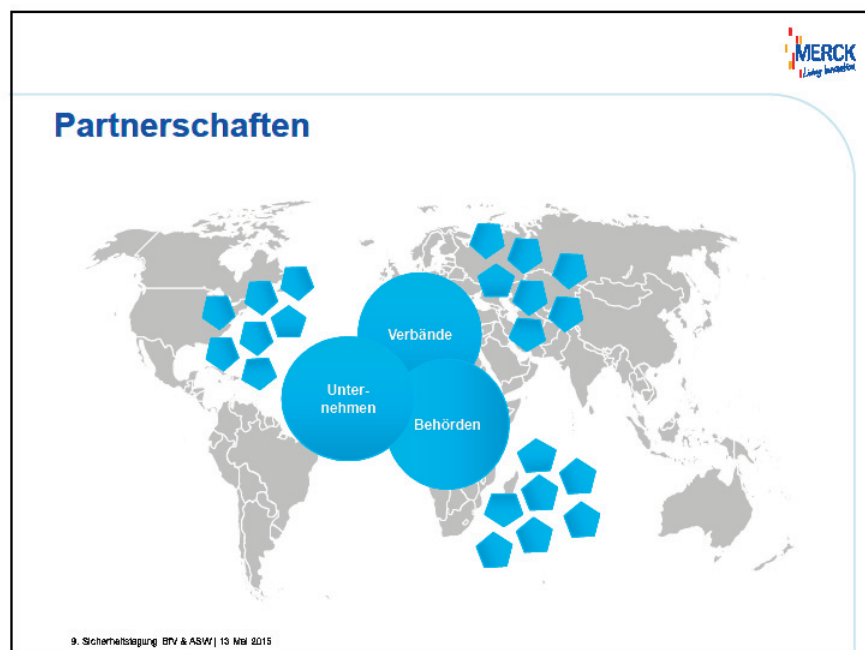
**Verantwortung für unsere Mitarbeiter**

Die Mitarbeiter sind für ein Unternehmen die Grundlage des Erfolgs. Sie nehmen in unserem unternehmerischen Handeln dementsprechend eine zentrale Rolle ein. Gemäß unseren Unternehmenswerten leben wir bei Merck eine Kultur der gegenseitigen Wertschätzung und des Respekts. Wir wollen zum Unternehmenserfolg beitragen, indem wir die am besten geeigneten Mitarbeiter einstellen, fördern und motivieren. Einen strategischen Schwerpunkt legen wir daher auf die Themen Talententwicklung, Vergütung und Leistungsmanagement. Darüber hinaus wollen wir die Vielfalt unter unseren Mitarbeitern fördern (ausführliche Informationen im Kapitel „Mitarbeiter“ ab Seite 77).

**Quelle: Merck Geschäftsbericht 2014**

- ▶ Talententwicklung
- ▶ Performance Management
- ▶ Diversity
- ▶ Arbeitssicherheit
- ▶ Arbeitszeitmodelle
- ▶ Aus- und Weiterbildung
- ▶ Nachwuchsförderung
- ▶ Leistungsvergütung

9. Sicherheitsagung BRV & ASW | 13 Mai 2015







## Ansätze für die Zukunft

Der Blick nach vorne



- ▶ Balance: Strafrecht – Zivilrecht – Arbeitsrecht
- ▶ Informationsaustausch mit Behörden und in Netzwerken intensivieren & koordinieren
- ▶ Zertifikatprogramme belasten Unternehmen einseitig
- ▶ Befugnisse müssen den steigenden Herausforderungen angepasst werden
- ▶ Reaktionsgeschwindigkeit von Behörden und Firmen auf neue Bedrohungen erhöhen
- ▶ Gefahren durch ‚Social Media‘

9. Sicherheitskongress BRV & ASWI | 13. Mai 2015

## „Background Checks – eine effektive Präventivmaßnahme beim recruiting“


Eckhard Neumann, Geschäftsführer, Signum Consulting GmbH

### BACKGROUND CHECKS

# SIGNUM

Consulting

Eine effektive Präventivmaßnahme beim Recruiting  
9. BfV/ASW Sicherheitstagung „Innentäter“



Bildquelle: <http://goo.gl/YKAvpA>

**PES**  
Pre-Employment Screening

SIGNUM Consulting GmbH | Eckhard Neumann  
9. BfV/ASW Sicherheitstagung „Innentäter“ | 13. Mai 2015

### FALLBEISPIELE

- DAX30-Unternehmen
  - Bewerbung als „IT Internal Auditor“
  - Ergebnis: **Krimineller Background im Ausland**
- Deutsches Mittelstandunternehmen
  - Bewerbung als „HR Manager“
  - Ergebnis: **Abschlüsse gefälscht**
- Chemiekonzern
  - Bewerbung als „Sicherheitsingenieur“
  - Ergebnis: **Universität existiert nicht (Diploma Mills)**



Bildquellen: <http://goo.gl/3rmZYf>; <http://goo.gl/HKx9IG>; <http://goo.gl/n2ed8h>

**SIGNUM**  
Consulting

## VON DER SCHÖNFÄRBEREI ZUM BETRUG

§267 StGB Urkundenfälschung  
§263 StGB Betrug  
§132a StGB Missbrauch von Titeln, Berufsbezeichnungen und Abzeichen

Was ist Schönfärberei? Wann fängt Betrug an?

Schokoladenseiten herausarbeiten Aufwertung der eigenen Angaben Schwächen kaschieren	Falschangaben z.B. Berufsbezeichnungen Stellenbezeichnungen Verantwortlichkeiten	Kauf von Dokortiteln und Diplomen Urkunden- oder Unterschriftenfälschung
--	---	---

3 **SIGNUM**  
Consulting

## WAS BEGÜNSTIGT FÄLSCHUNG UND BETRUG?

### Veränderungen im Bewerbungsverfahren

- Digitalisierung
- Internetpräsenz der Firmen und Bildungseinrichtungen
- Onlinebewerbungen
- Kandidatenpool
- Technische Möglichkeiten

### Internationalisierung des Arbeitsmarktes

- Globalisierung verändert Anforderungen
- entsprechender Druck auf Bewerber
- Diploma Mills
- International variierende Berufsbezeichnungen
- Sprachbarrieren

4 **SIGNUM**  
Consulting

## POTENTIELLE SCHÄDEN FÜR IHR UNTERNEHMEN

- **Finanziell**

Neueinstellung eines Managers mit

- Zwei-Jahres Vertrag
- Dienstwagen
- Hohem Gehalt (ca. 300.000 EUR/Jahr)



Nach 3 Monaten:

- Feststellung: Bewerbungsbetrug**
- Freistellung bis zum Ablauf des Vertrages
- Direkter Schaden: min. 600.000 EUR**
- Zzgl. Indirekte Schäden

- Zeitverlust durch Neubesetzung
- **Reputationsschaden**
- Haftungsrisiken
- Kundenbeziehungen leiden
- Sinkende Arbeitsmoral

5

## RECRUITMENT-PROZESS UND PES

PES ist die Überprüfung von relevanten Bewerbungsdaten auf Ihre Richtigkeit.



**Ausschreibung:**  
Operations Manager

**Aufgaben:**  
Erstellen von Angeboten  
Koordination  
Fachliche Führung

**Auswahl:**  
Passt die Bewerbung  
auf das gesuchte Profil?

10 Bewerber von 150

**Einladung der Auswahl:**  
Persönl. Kennenlernen  
event. Assessment Center  
event. 2. Gespräch

3 Bewerber von 10

3 Bewerber von 10

1 Bewerber von 3

**PRE-EMPLOYMENT SCREENING**

- 1 Bewerbungssystem: Hinweis auf Referenzverifizierung als Teil des Einstellungsprozesses
- 2 Einverständniserklärung wird vorgelegt und Kandidat aufgeklärt
- 3 Referenzen der Kandidaten überprüfen, die es in die engere Auswahl geschafft haben

6

## WAS WIRD VERIFIZIERT?



- **Standard:**
  - Bildungsabschlüsse
  - Arbeitsverhältnisse
  - Praktika
  - Selbstständigkeit
  - Referenzen
- **Executive:**
  - Aktuelle Firmenbeteiligungen
  - Kreditwürdigkeit
  - Media Reputation
  - Negativinformationen / Sanktionslisten

7

**SIGNUM**  
Consulting

## INDIVIDUAL COMPLIANCE CHECK



- Abgleich mit > **1.300 internationalen Negativlisten**, z.B.
  - Sanktionslisten
  - Watch Lists
  - Korruptionslisten
  - Anti-Terror-Listen
  - Embargolisten
  - PEP-Listen



8

**SIGNUM**  
Consulting

## WIE WIRD VERIFIZIERT?



- Verifizierungen durch:
  - **Experten**
    - Persönlicher Kontakt
    - Zugriff auf interne Datenbank (> 5.700 Einträge weltweit)
      - Hochschulen
      - Arbeitgeber
      - Behörden
    - Eigenrecherche
    - Übersetzungen
  - **Internationales Partnernetzwerk**
  - **Kostenpflichtige Compliance-Datenbanken**

9

**SIGNUM**  
Consulting

## RECHTLICHE ASPEKTE

Bundesdatenschutzgesetz



### EINVERSTÄNDISERKLÄRUNG

#### **Muss schriftlich erteilt werden**

- ✓ Darf nicht im „Kleingedruckten“ versteckt werden
- ✓ Ist optisch besonders hervorzuheben

#### **Was soll daraus ersichtlich sein?**

1. Die Art der gespeicherten Daten
2. Der Empfänger oder die Kategorien von Empfängern dieser Daten
3. Der konkrete Zweck der Speicherung

10

**SIGNUM**  
Consulting

„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN

## FAZIT



- Besetzung der Stelle mit bestem Bewerber
- HR-Prozesse
  - Hohe Transparenz für Bewerber und Arbeitgeber
  - Einheitliche Prozesse
  - Kosten einer Fehlbesetzung senken
- Sicherheit, Gewissheit & Transparenz
- Haftungsrisiken senken
- Reputationsschäden vermeiden
- **Internationale Compliance-Standards**

11

**SIGNUM**  
Consulting

## VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!



SIGNUM Consulting GmbH

Rungestraße 19 | 10179 Berlin | Germany  
Tel.: +49 30 278736 – 10  
Fax.: +49 30 278736 – 22  
Email: E.Neumann@signum-consult.com

Web: [www.signum-consult.com](http://www.signum-consult.com) | [www.pre-employment-screening.com](http://www.pre-employment-screening.com)



12

**SIGNUM**  
Consulting

## „Identifizierung und Steuerung personeller Risiken mit Business Profiling“

Ralf Kopp, Geschäftsführer, KOPP GmbH



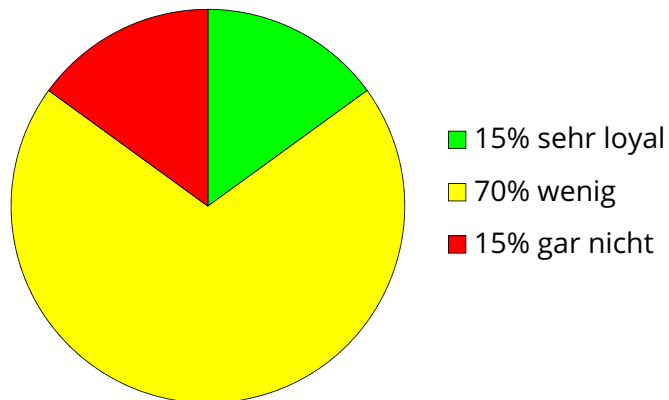
**Business Profiling**



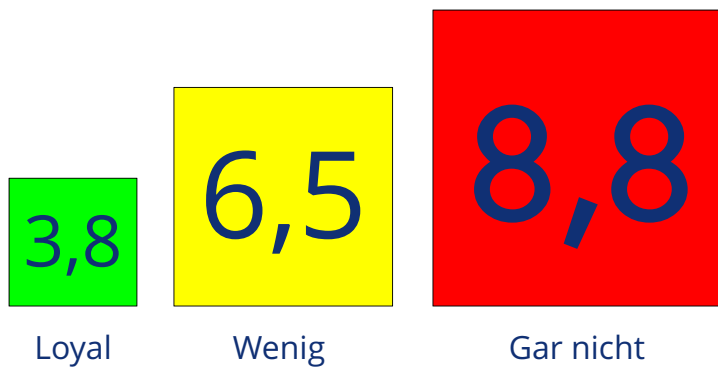
**Innentäter**



## Loyalität



## Fehltage



## Innentäter

sind immer illoyal

## Loyalität basiert auf

- Menschenkenntnis
- Kommunikation
- Führung

## Zusammenhang

Mangelhafte Steuerungsfähigkeiten



Wenig Loyalität



Viele Innentäter

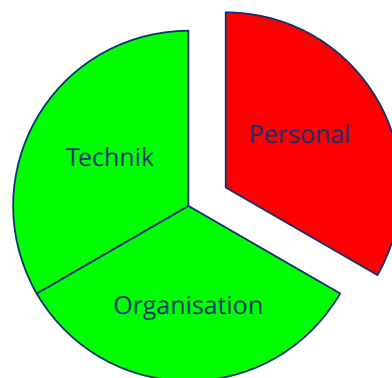
## Die Unternehmen

produzieren ihre Innentäter selbst

## Ist Loyalität

in Ihrem Unternehmen ein Thema?

## TOP



## Respekt

Deutschland	Frankreich	USA
Respekt	Respekt	Respekt
Zeit für Privatleben	Zeit für Privatleben	Kompetente Chefs
Interessante Arbeit	Interessante Arbeit	Zeit für Privatleben
Grundgehalt	Kompetente Chefs	Arbeit, die Werte schafft

## Respectare

genau hinsehen

## Neurowissenschaften

„Keiner kann anders, als er ist“

Prof. Wolf Singer

## Eigenschaften sind Hardware

## Sigmund Freud

„Unsere Persönlichkeit  
dringt uns jeden Tag aus allen Poren“

## Criminal Profiling

Empirische Täterprofile

## Systematischer Prozess

der subjektive Beurteilungen  
weitgehend ausschaltet

## Objektive Merkmale

- Lebenslauf
- Beobachtungen
- Interviews
- Internetrecherche



## Ausbildung

Jede Entscheidung sagt etwas aus

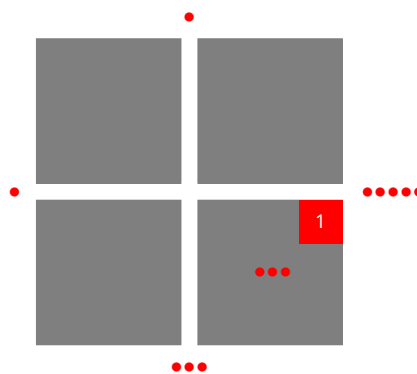
## Kommunikationsebene

- Sachebene
- Beziehungsebene
- Appellebene
- Selbstkundgabeebene

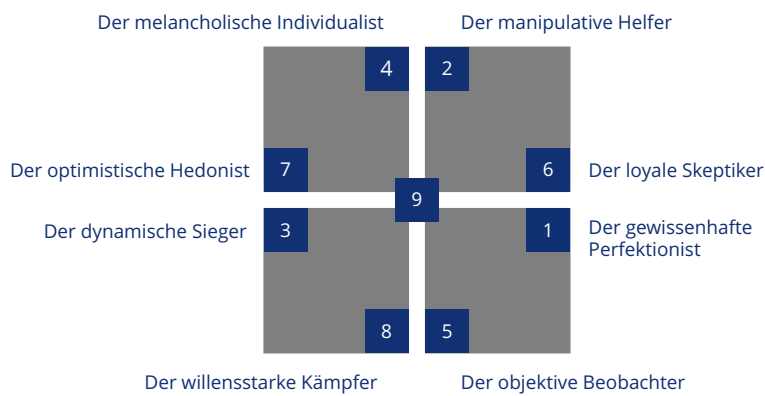
## Quantitative Sprachanalyse



## Profiling-Kreuz



## 9 Typen



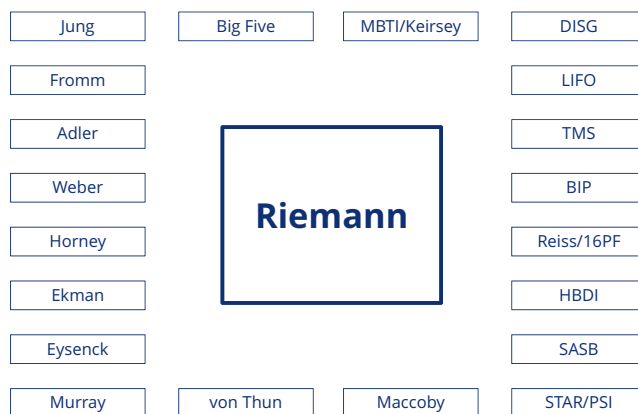
## Eigenschaften

- Loyalität
- Integrität
- Regeltreue
- Risikoneigung

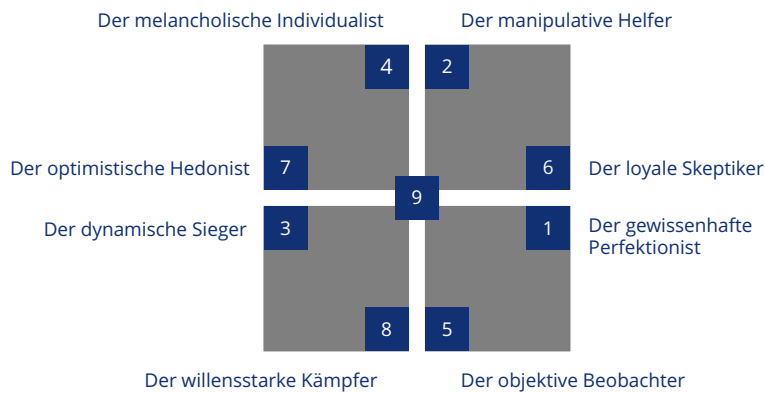
## Mehr Eigenschaften

- Verhalten in Konflikten
- Verhalten in Verhandlungen
- Trigger

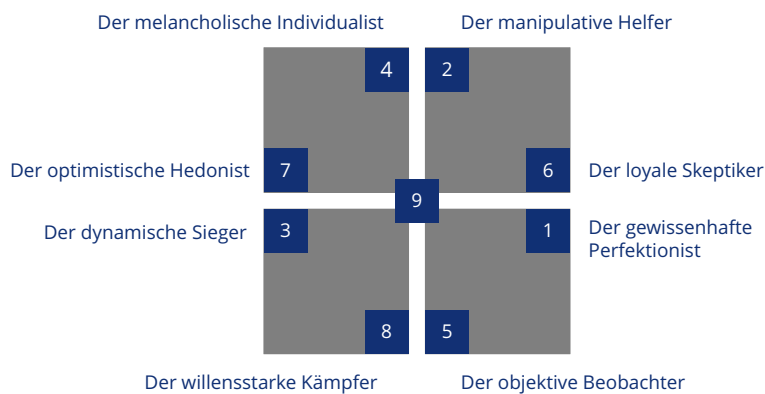
## Typologien und Strukturmodelle



## Beispiele Berufe



## Beispiele Personen



## Unterschiede 1 und 3

<u>Eigenschaft</u>	<u>Typ 1</u>	<u>Typ 3</u>
Loyalität	★★★★☆☆	★☆☆☆☆
Integrität	★★★★★★	★☆☆☆☆
Regeltreue	★★★★★★	★☆☆☆☆
Risikoneigung	★☆☆☆☆	★★★★★★

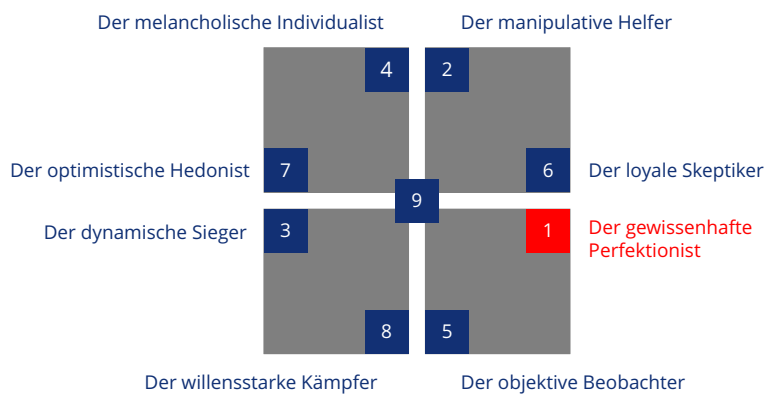
## Spezielle Situationen

Dilemma der 1

## Unterschiede 1 und 6

Eigenschaft	Typ 1	Typ 6
Loyalität	★★★★☆☆	★★★★★★
Integrität	★★★★★★	★★★★☆☆
Regeltreue	★★★★★★	★★★★★★
Risikoneigung	★☆☆☆☆	★☆☆☆☆

## Snowden



# IT-Admin

Kündigung  
↓  
Illegale Datenzugriffe

KOPP GMBH Business Profiling © 2015 KOPP GMBH 33

# IT-Admin

	4	2	
7	9	6	Der loyale Skeptiker
3		1	Der gewissenhafte Perfektionist
	8	5	
	Der willensstarke Kämpfer	Der objektive Beobachter	

KOPP GMBH Business Profiling © 2015 KOPP GMBH 34



## Gleichwertigkeit

Alle Strukturen sind gleichwertig.  
Nur anders.

## Ähnlichkeitsfalle

Wir mögen die Menschen,  
die so sind, wie wir selbst sind

# Psychopathen

im medizinischen Sinne  
nach Prof. Robert Hare

# Hare-Skala

0-40

## Psychologisches Inventar

- Charme
- Charisma
- Reduzierte Emotionen, insbesondere
  - reduzierte Angst
  - reduziertes Mitgefühl
- Hohes Einfühlungsvermögen
- Hohes Beeinflussungsvermögen
- Kaltblütigkeit
- Fokussierung
- Mentale Härte
- Durchsetzungsvermögen
- Rücksichtslosigkeit

## Häufigkeit

5%

## Funktionale Psychopathen

Top-Performer

## Dysfunktionale Psychopathen

- Verantwortungslosigkeit
- Gewissenlosigkeit
- Dysfunktionale Gewalt
- **Keine Kontrolle**

## Champions League

der Innentäter

## 1. Bewusstsein entwickeln

Persönlichkeitsstrukturen

Menschenkenntnis    Kommunikation

Führung    Respekt    Loyalität

Innentäter

## 2. Zusammenhang

sichtbar machen

## 3. Risiken identifizieren

- Illoyale Mitarbeiter
- Loyale Mitarbeiter in Konflikten
- Dysfunktionale Psychopathen

## 4. Mitarbeiter in Konflikten

unterstützen

## 5. Führungskräfte trainieren

- Menschenkenntnis
- Kommunikation
- Führung

## 6. Psychopathen

Entfernen Sie  
dysfunktionale Psychopathen

## Wirtschaftlichkeit

### Investition in

- Menschenkenntnis
- Kommunikation
- Führung

### Schäden durch

- Straftaten
- Andere schädigende Handlungen



## Trainings in Business Profiling



- Inhouse für die Mitarbeiter von Sicherheitsbehörden und Unternehmen
- Extern für Einzelbucher (nur für einen eingeschränkten Personenkreis)



**Vielen Dank!**


[www.koppgmbh.de](http://www.koppgmbh.de)

## „Wirtschaftsschutzgrundhandbuch – Vorhang auf für die ersten Bausteine“

Prof. Timo Kob, Vorstandsmitglied, ASW Bundesverband



 EUROPÄISCHE UNION  
Europäischer Fonds für  
regionale Entwicklung

### Forschungsprojekt WISPER

„Wirtschaftsgrundschutz“ als Werkzeug zum Schutz vor Spionage und Sabotage

Prof. Timo Kob

## 720° Wirtschaftsschutz

**HISOLUTIONS** **ASW Bundesverband**

- Spionage und Sabotage sind nicht nur für Konzerne, sondern auch und gerade für den Mittelstand – als dem „Rückgrat“ der deutschen Wirtschaft – eine reale Bedrohung
- Auch wenn derzeit ein Großteil der Aufmerksamkeit dem Thema Cyber Security gilt, so finden Angriffe auf deutsche Unternehmen weiterhin auch über „klassische“ Wege statt
- Die doppelte Herausforderung heißt also:

**Allen Gefährdeten für ALLE Bedrohungen Schutzmöglichkeiten bieten!**



Forschungsprojekt WISPER – Folie 3

## Das Ziel: Ein Paradoxon auflösen!

**HISOLUTIONS** **ASW Bundesverband**

- Für das – vermeintlich – neue Angriffsziel IT gibt es seit 20 Jahren ein erfolgreiches Hilfsmittel: Den IT-Grundschutz des BSI
- Für die „klassischen“ Angriffsziele wie Mensch, Infrastrukturen und Prozesse gibt es dies nicht
- Ziel von WISPER ist es, diese Lücke zu schließen!



Forschungsprojekt WISPER 22. Juni 2015 – Folie 4

## Das Ziel: Ein Paradoxon auflösen!



- Für das – vermeintlich – neue Angriffsziel IT gibt es seit 20 Jahren ein erfolgreiches Hilfsmittel:  
Den IT-Grundschutz des BSI
  
- Für die „klassischen“ Angriffsziele wie Mensch, Infrastrukturen und Prozesse gibt es dies nicht.
  
- Ziel von WISPER ist es, diese Lücke zu schließen!



Forschungsprojekt WISPER22. Juni 2015 – Folie 5

## Die Projektpartner





- Bundesverband für Sicherheitsverantwortliche in der Wirtschaft und Verantwortliche in der Sicherheitswirtschaft
- Scharnier zwischen Wirtschaft und Behörden.
- Bringt so Staat, Wirtschaft und Anbieter zusammen



- Beratungsspezialist für Informationssicherheit und Wirtschaftsschutz
- Führender Experte für den IT-Grundschutz und Rahmenvertragspartner des BSI
- Derzeit vom BSI mit der Neugestaltung des IT-Grundschutzes beauftragt

Unterstützende Behörden:



Bundesamt für Verfassungsschutz



Bundesamt für Sicherheit in der Informationstechnik

Forschungsprojekt WISPER22. Juni 2015 – Folie 6

## Vorgehen, Ziele und Wünsche



- Nicht nur Mitgliedsverbände der ASW sind eingeladen mitzuwirken, sondern auch externe Fachleute und Verbände
- ASW und HiSolutions wollen keinen „eigenen“ Standard schaffen und auch nicht „das Rad neu erfinden“
- Ziel ist die Diskussion und Konsensfindung für angemessene Mindestanforderungen, Empfehlungen und Hilfsmittel
- Analog zum IT-Grundschutz soll das Ergebnis abschließend kostenfrei zur Verfügung gestellt werden – idealerweise wieder in Analogie zum IT-Grundschutz zumindest mit Beteiligung einer staatlichen Institution

## Die Ebenen des Wirtschaftsgrundschutzes



### **Ebene 1 – Standards**

Hier wird die allgemeine Methodik (u.a. Auswahl von Bausteinen/Maßnahmen, Reifegrad) definiert und mögliche Ablauf- und Aufbauorganisationen (Managementsystem) einer integrierten Sicherheitseinheit beschrieben.

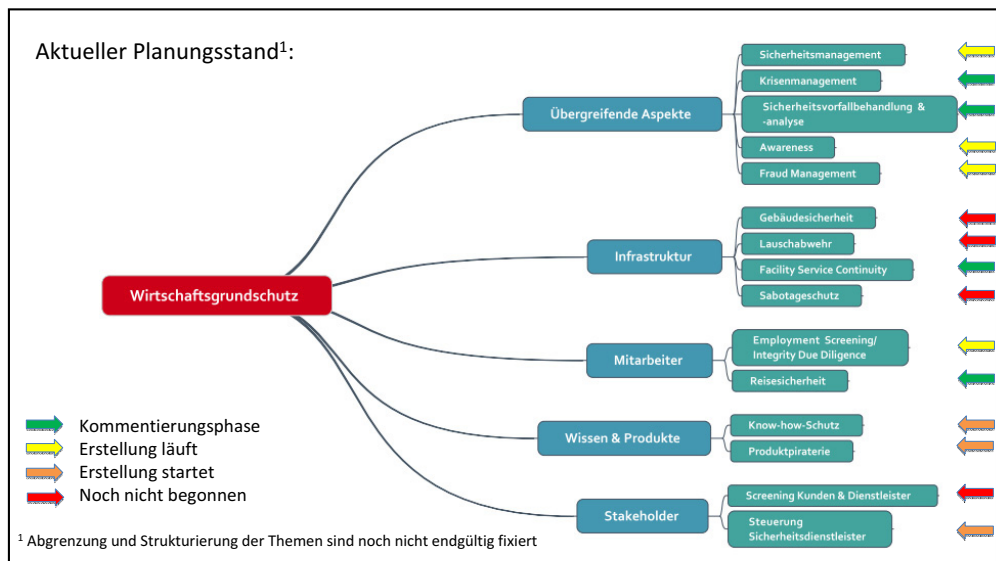
### **Ebene 2 – Bausteine**

Bausteine fassen konkrete Maßnahmen zu einem Themenkomplex zusammen. Die Maßnahmen werden nach ihrer Bedeutung kategorisiert/priorisiert.



### **Ebene 3 – Vertiefungsdokumente**

Bereits bestehende Dokumente, Guidelines, Bücher und Normen werden als Referenzen aufgenommen und verhindern so redundante Regelung.

„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN



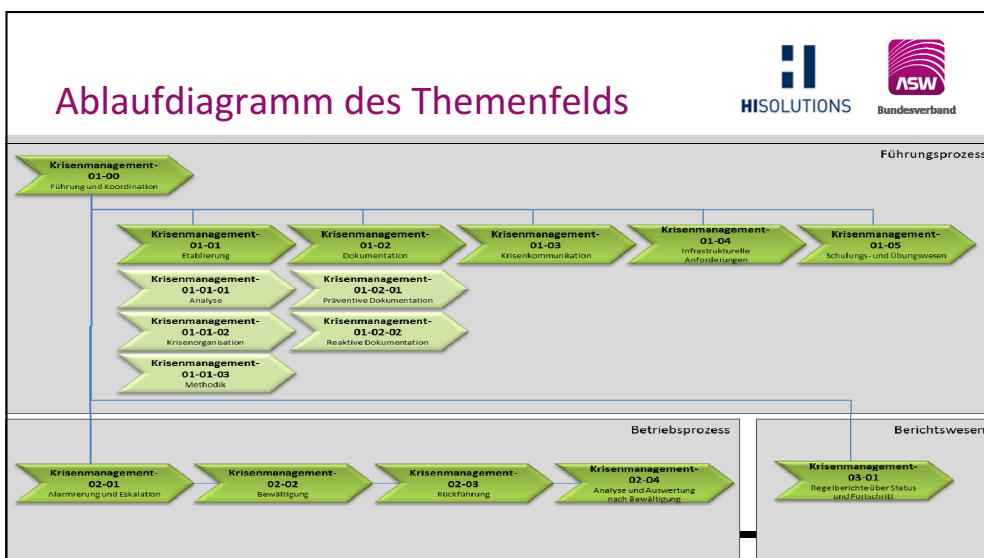
**Beispielbaustein Krisenmanagement**



---

Präsentationstitel in Kopf Fußzeile 22. Juni 2015 – Folie 10

„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN



## M3 Aufbau eines Krisenstabs (A)

Inhalt	Kurzbeschreibung
Charakter	<ul style="list-style-type: none"> <li>▪ besondere Aufbauorganisation mit besonderen Befugnissen</li> <li>▪ zentrales Krisenmanagementorgan mit allen erforderlichen abteilungsübergreifenden Kompetenzen</li> </ul>
Aufgaben	<ul style="list-style-type: none"> <li>▪ Erstellen und Bewerten des Lagebilds</li> <li>▪ Entwickeln und Bewerten von Handlungsoptionen</li> <li>▪ Steuern der Bewältigungsmaßnahmen</li> <li>▪ Koordinieren der Zusammenarbeit mit Dritten</li> <li>▪ Organisieren der Stabsarbeit</li> <li>▪ Organisieren der internen und externen Krisenkommunikation</li> </ul>
Besetzung	<ul style="list-style-type: none"> <li>▪ Kernteam</li> <li>▪ Erweiterter Krisenstab</li> <li>▪ Unterstützende Funktionen</li> </ul>

Präsentationstitel in Kopf- Fußzeile
22. Juni 2015 – Folie 13

## M10 Erstellen eines Krisenplans (A)




Inhalt	Kurzbeschreibung
Charakter	<ul style="list-style-type: none"> <li>▪ reaktives und einsatzorientiertes Dokument</li> <li>▪ enthält die wichtigsten Informationen zur systematischen Bewältigung von Krisenereignissen</li> </ul>
Themen	<ul style="list-style-type: none"> <li>▪ Erstmaßnahmen</li> <li>▪ Lagebearbeitung</li> <li>▪ Führung</li> <li>▪ Deeskalation und Rückführung</li> </ul>
Weitere Informationen	<ul style="list-style-type: none"> <li>▪ Agenda für das erste Zusammentreffen des Krisenstabs</li> <li>▪ Kompetenzen und Verantwortlichkeiten</li> <li>▪ Kontaktinformationen</li> <li>▪ Verfahren zur methodischen und Szenario-spezifischen Arbeit</li> <li>▪ Vorlagen für Krisenstabsprotokoll, Lagebericht, Visualisierung</li> </ul>

Präsentationstitel in Kopf- Fußzeile
22. Juni 2015 – Folie 14





## M22 Erstellen eines Krisenkommunikationsplans (A)




Inhalt	Kurzbeschreibung
Charakter	<ul style="list-style-type: none"> <li>▪ vorrangig reaktives Dokument</li> <li>▪ beschreibt die Kontrolle und Steuerung der Informationsflüsse</li> </ul>
Themen	<ul style="list-style-type: none"> <li>▪ Analyse der Interessengruppe</li> <li>▪ Medienbeobachtung und -management</li> <li>▪ Entwicklung der Krisenkommunikationsstrategie</li> <li>▪ Interne und externe Kommunikation</li> </ul>
Weitere Informationen	<ul style="list-style-type: none"> <li>▪ Grundlagen Krisenkommunikation und Kommunikationsregeln</li> <li>▪ Kommunikationsmittel und -materialien</li> <li>▪ Liste der Interessensgruppen (Stakeholder-Matrix)</li> <li>▪ Vorbereitete Inhalte (z.B. Mustertexte, FAQ)</li> <li>▪ Kontaktliste zu Medien/Experten</li> </ul>

Präsentationstitel in Kopf- Fußzelle
22. Juni 2015 – Folie 15

## Übersicht der Maßnahmen des Bausteins

A – Erstmaßnahmen	B – Basismaßnahmen	C – erweiterte Maßnahmen
<ul style="list-style-type: none"> <li>M1 Identifikation von Bedrohungen und Gefährdungen mit besonderem Krisenpotential</li> <li>M3 Aufbau eines Krisenbewältigungsgremiums</li> <li>M4 Definition der Kompetenzen, Verantwortlichkeiten und Aufgaben</li> <li>M10 Erstellen eines Krisenplans</li> <li>M15 Bereitstellen geeigneter Räumlichkeiten für den Krisenstab</li> <li>M17 Definieren der Verfahrensweisen für die Lagebeurteilung und -bearbeitung sowie Entscheidungsfindung</li> <li>M18 Definieren der Verfahrensweisen für die Dokumentation</li> <li>M22 Erstellung eines Krisenkommunikationsplans</li> <li>M23 Festlegen der Rollen und Definition der Kompetenzen, Verantwortlichkeiten und Aufgaben der Krisenkommunikation</li> <li>M25 Definition der Kommunikationsmittel und -materialien</li> <li>M27 Identifizieren des Schulungsbedarfs</li> <li>M28 Erstellen eines Schulungskonzepts</li> <li>M30 Durchführen von Schulungen</li> <li>M34 Identifikation und Erstellung der erforderlichen Übungsdokumentation</li> </ul>	<p>Maßnahmen A</p> <p>+</p> <ul style="list-style-type: none"> <li>M2 Entwicklung einer geeigneten Organisationsstruktur</li> <li>M5 Erstellen einer Leitlinie und Übernahme der Gesamtverantwortung</li> <li>M6 Erstellen eines Rahmenwerks</li> <li>M8 Erstellen eines Alarmierungskonzepts</li> <li>M11 Erstellen eines Alarmierungsplans</li> <li>M12 Entwickeln von Szenario-spezifischen Checklisten</li> <li>M19 Definieren der Verfahrensweisen für die Visualisierung</li> <li>M21 Identifikation und Analyse der Interessengruppen</li> <li>M24 Festlegen eines Verfahrens für die Medienbeobachtung</li> <li>M26 Aufbau einer Darksite / Shadowsite</li> <li>M29 Erstellen des erforderlichen Schulungsregelwerks</li> <li>M31 Entwicklung eines Übungsprogramms</li> <li>M32 Definition eines standardisierten Übungszyklus</li> <li>M33 Definition der erforderlichen Übungsrollen</li> </ul>	<p>Maßnahmen A und B</p> <p>+</p> <ul style="list-style-type: none"> <li>M7 Erstellen eines Krisenhandbuchs</li> <li>M9 Erstellen einer Geschäftsordnung für den Krisenstab</li> <li>M13 Erstellen von Rollenkarten</li> <li>M14 Bereitstellen aller notwendigen Vorlagen und Werkzeuge</li> <li>M16 Definieren der Verfahrensweisen zur Erarbeitung der Krisenmanagementstrategie</li> <li>M20 Definieren der Verfahrensweisen für den Schichtwechsel und die Lageübergabe</li> </ul>

## Die ASW bedankt sich für Ihre Aufmerksamkeit

Allianz für Sicherheit in der Wirtschaft e.V.  
Zieher Business Center  
Rosenstraße 2  
10178 Berlin  
[www.aswbundesverband.de](http://www.aswbundesverband.de)  
+49 (0) 30 200 77 200



## „Spionage durch Innentäter, so einfach war es noch nie..“

Frank Eckhardt, Leiter Lauschabwehr, Deutsche Telekom AG



ERLEBEN, WAS VERBINDET.



### SCHUTZ VOR SPIONAGE/LAUSCHANGRIFFEN Innentäter, Kenne ich keine

Outsourcing = Abgabe von Unternehmensaufgaben und -strukturen



Informations-  
technologie  
(IT-Service,  
Administrator)



Dienstleistung  
(Wachdienst,  
Reinigung)



Handwerk  
(Maler,  
Elektriker,  
Installateur)



Berater,  
Vertrieb,  
Leiharbeiter

Setzen Sie langjährige Mitarbeiter/Innen bzw. vertrauenswürdige Personal ein!



ERLEBEN, WAS VERBINDET.

ASW und BVV – „Innentäter“ eine unterschätzte Gefahr

13.05.2015

Seite  
2



ERLEBEN, WAS VERBINDET.

## SCHUTZ VOR SPIONAGE/LAUSCHANGRIFFEN BILLIG ABER GEFÄHRLICH

Wie viele Treffer bekommen Sie bei einer „Googlesuche“ nach Spyshop? 600.000!



Einige Exponate, die schnell und einfach von Innentätern platziert werden können.



ERLEBEN, WAS VERBINDET.

ASW und BfV – „Innentäter“ eine unterschätzte Gefahr

13.05.2015

Seite 3

## SCHUTZ VOR SPIONAGE/LAUSCHANGRIFFEN SICHERHEIT muss von oben gelebt werden

Bei sensiblen Informationen ist ein gewisses Maß an Kontrolle unerlässlich.  
Schutzmaßnahmen sind umso wirksamer, je weniger sie bekannt sind.



Schützen Sie das gesprochene Wort bzw. Ihr Geschäftsgeheimnis!



ERLEBEN, WAS VERBINDET.

ASW und BfV – „Innentäter“ eine unterschätzte Gefahr

13.05.2015

Seite 4



ERLEBEN, WAS VERBINDET.

## SCHUTZ VOR SPIONAGE/LAUSCHANGRIFFEN WAS EINEN PROFESSIONELLEN SWEEP AUSMACHT

Räumlichkeiten in denen Geschäftsgeheimnisse ausgetauscht werden,  
sind auf Abhörsicherheit zu überprüfen.

Bestandteile einer Lauschatwehrüberprüfung (Sweep):

- ✓ Funktechnische Untersuchung
- ✓ Glas transmissionsmessung
- ✓ Halbleiterdetektion
- ✓ Leitungsuntersuchung
- ✓ Röntgenuntersuchung
- ✓ Visuelle Untersuchung
- ✓ Wärmebildanalyse



Bewahren Sie sich vor Informationsverlusten und sichern Sie Ihr Business!



ERLEBEN, WAS VERBINDET.

ASW und BIV – „Innentäter“ eine unterschätzte Gefahr

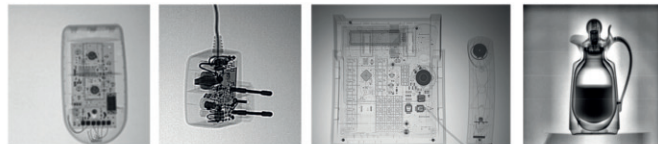
13.05.2015

Seite 5

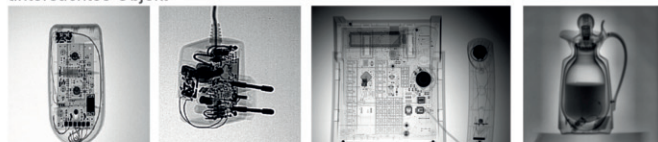
## SCHUTZ VOR SPIONAGE/LAUSCHANGRIFFEN VERSCHAFFEN SIE SICH DEN DURCHBLICK

Haben Sie die Manipulationen gleich gefunden?

Referenzbild



untersuchtes Objekt



ERLEBEN, WAS VERBINDET.

ASW und BIV – „Innentäter“ eine unterschätzte Gefahr

13.05.2015

Seite 6

„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN



ERLEBEN, WAS VERBINDET.

## Kontakt

DEUTSCHE TELEKOM AG

**Frank Eckhardt**  
Group Security Services  
Eavesdropping Protection & Security Checks  
Mina-Rees-Straße 8,  
64295 Darmstadt  
+49 6151 583 1550 (Tel.)  
+49 151 628 19 299 (Mobil)  
Frank.Eckhardt@Telekom.de (E-Mail)



ERLEBEN, WAS VERBINDET.

## „Detektion aus der Praxis – Beispiele national/international agierender Unternehmen“



Sandra Wippermann, Gesellschafterin, Detektei – Holler GmbH

DETEKTEI-HOLLER GmbH

### 9. Sicherheitstagung des BfV und der ASW

**„Innentäter“  
eine unterschätzte Gefahr in Unternehmen**

Sandra Wippermann  
13. Mai 2015 in Berlin

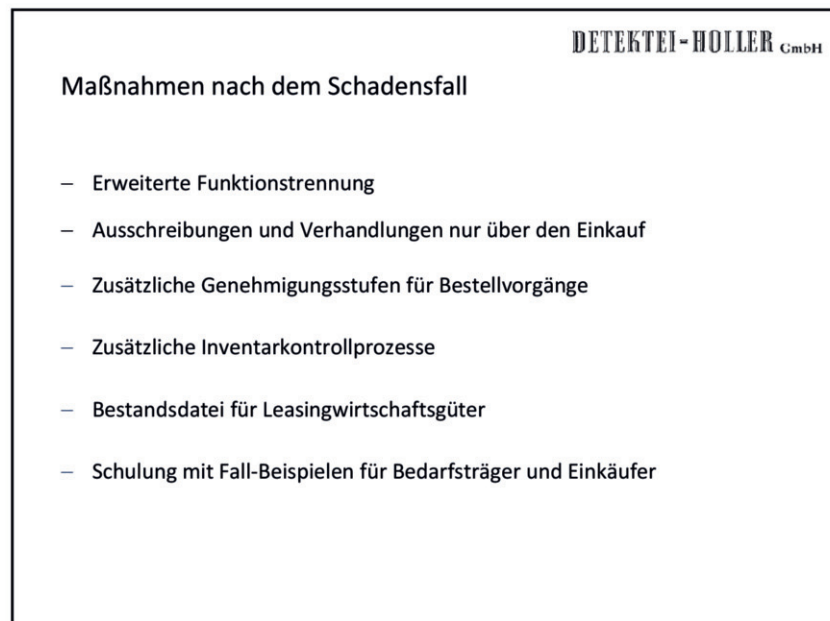
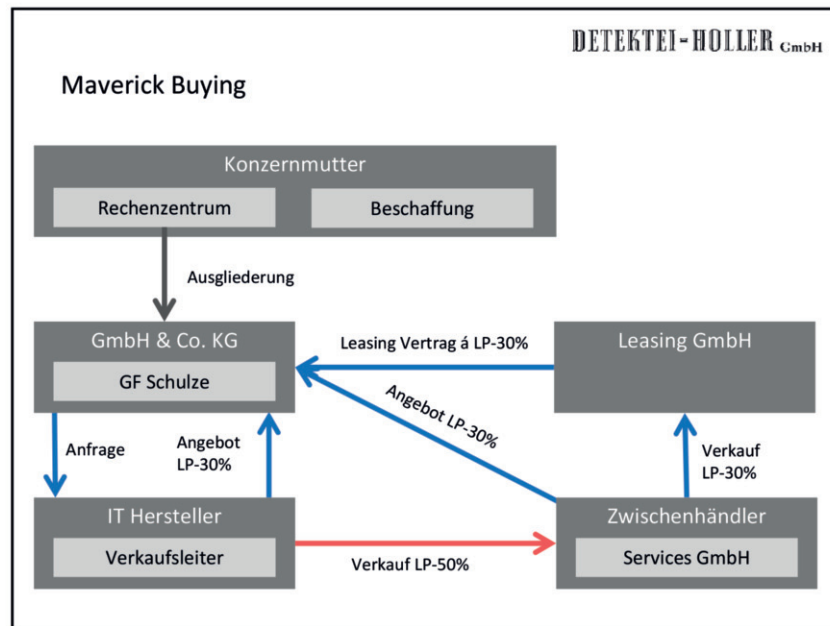


DETEKTEI-HOLLER GmbH

Erstes Fallbeispiel

### Maverick Buying:

Einkauf durch Außerkraftsetzung  
standardisierter Beschaffungswege  
eines leitenden Angestellten





DETEKTEI-HOLLER GmbH

Zweites Fallbeispiel

Produkte unserer Auftraggeberin  
wurden auf dem europäischen Markt  
weit unter Preis angeboten.

Es bestand Fälschungsverdacht.

**Sandra Wippermann**

DETEKTEI – HOLLER GMBH  
Beckhausstrasse 168  
D33611 Bielefeld  
T.+49 521 82160  
F.+49 521 874945  
s.wippermann@deho1.de  
www.detekteiholler.de

DETEKTEI-HOLLER GmbH

## Bildmaterial



„INNENTÄTER“  
EINE UNTERSCHÄTZTE GEFAHR IN UNTERNEHMEN



## **Impressum**

### **Herausgeber**

Bundesamt für Verfassungsschutz  
Referat Wirtschaftsschutz  
Merianstraße 100  
50765 Köln

Tel.: +49(0)221/792-0

Fax: +49(0)221/792-2915

wirtschaftsschutz@bfv.bund.de

**[www.verfassungsschutz.de](http://www.verfassungsschutz.de)**

### **Gestaltung und Druck**

Bundesamt für Verfassungsschutz  
Print- und Mediacenter

### **Bildnachweis**

© FotolEdhar - Fotolia.com

© Mike Minehan

© BfV/ASW

### **Stand**

Juli 2015

**Wirtschaftsschutz  
ist  
Teamwork**