Bundesamt für
Verfassungsschutz

ASW
Bundesverband

„Innentäter“ eine unterschätzte Gefahr in Unternehmen

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

T · ·

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

Inhaltsverzeichnis

„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 Personenkreise. 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 unterschätze 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 Auftragssituation eingeschleust wurde oder mit persönlich motivierter Schadensabsicht eindringt.

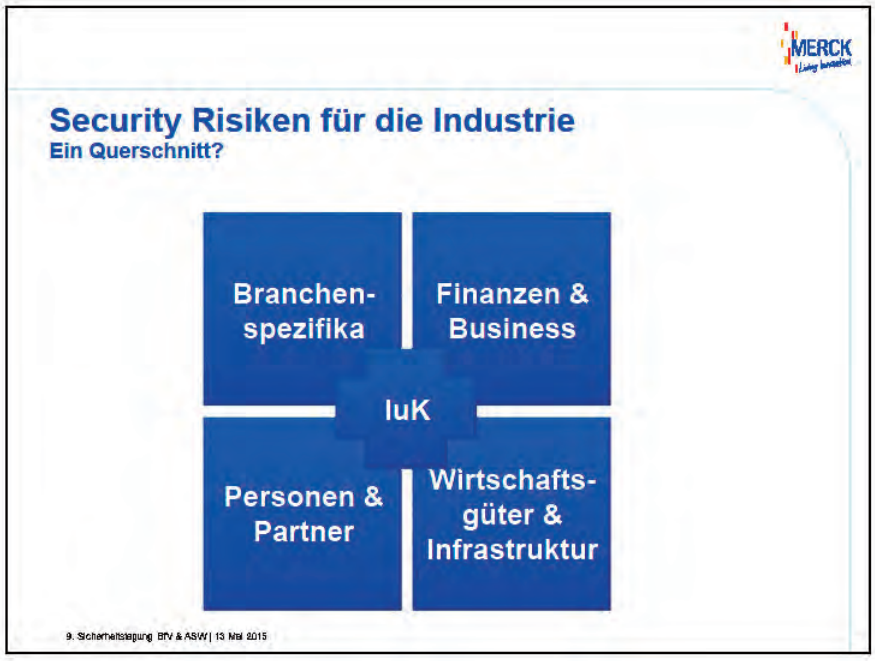
„Innentäter – eine unterschätzte Gefahr“

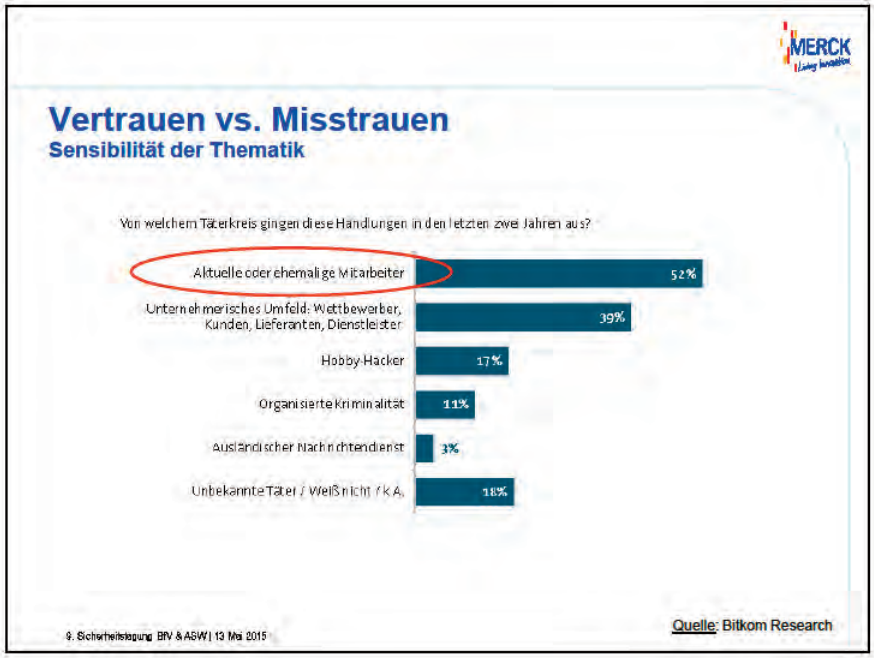
Andreas Maack, Chief Security Officer, Merck KGaA


MERCK
Was wir tun
Healthcare
Life Science
Performance Materials
Merck Serono, Consumer Health, Allergopharma, Biosimilars
Verschreibungspflichtige Medikamente, etwa gegen Krebs, Unfruchtbarkeit oder Multiple Sklerose, rezeptfreie Produkte bei Erkältung und Schmerzen, sowie Innovationen im Bereich Allergien und Biosimilars.
Merck Millipore
Innovative Instrumente und Labormaterialen für die Life-Science-Industrie, die Forschung und Biotech-Produktion einfacher, schneller und erfolgreicher machen.
Performance Materials
Spezialchemikalien für besondere Ansprüche wie Flüssigkristalle für Displays, Effektpigmente für Lacke und Kosmetik oder Hightech-Materialien für die Elektronik-Industrie.
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

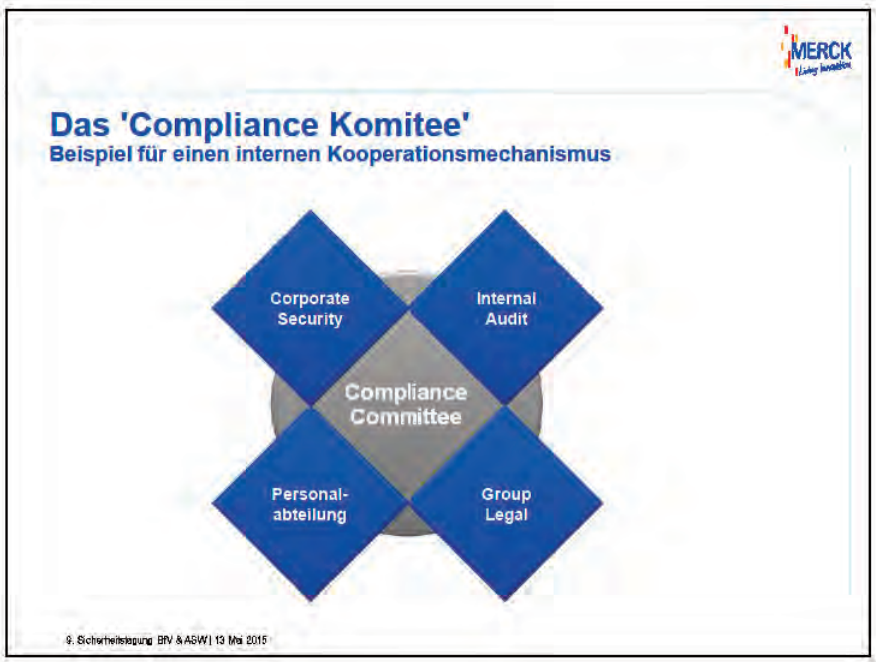

MERCK
Healthcare, Life Science & Performance Materials
1668 gegründet
66 Länder
39.000 Mitarbeiter
1,7 Mrd € für Forschung und Entwicklung 2014
11,3 Mrd € Umsatzerlöse 2014


MERCK
Wir sind im Familieneigentum
UND börsennotiert
Merck KGaA
Gesamtkapital 100,0%
Merck-Familie
Kapitalanteil 70,3%
Aktionäre
Grundkapital 29,7%
Im Familieneigentum seit 12 Generationen
Börsennotiert seit 1995 - Im DAX seit 2005
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

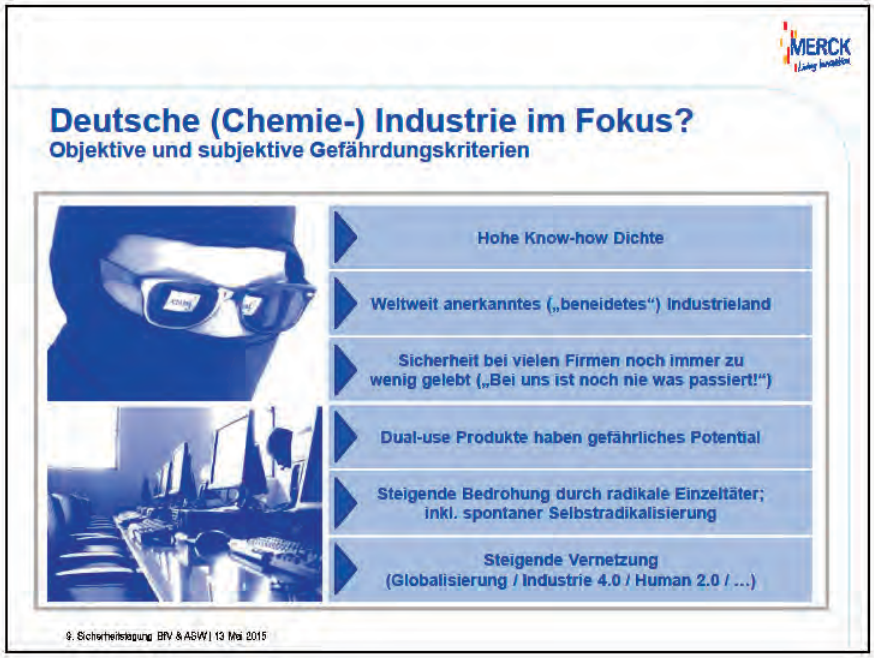

MERCK
Security Risiken für die Industrie
Ein Querschnitt?
Branchen-spezifika
Finanzen & Business
IuK
Personen & Partner
Wirtschafts-güter & Infrastruktur
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Vertrauen vs. Misstrauen
Sensibilität der Thematik
Von welchem Täterkreis gingen diese Handlungen in den letzten zwei Jahren aus?
Aktuelle oder ehemalige Mitarbeiter
52%
Unternehmerisches Umfeld: Wettbewerber, Kunden, Lieferanten, Dienstleister
39%
Hobby-Hacker
17%
Organisierte Kriminalität
11%
Ausländischer Nachrichtendienst
3%
Unbekannte Täter / Weiß nicht / k.A.
18%
9. Sicherheitstagung BfV & ASW | 13. Mai 2015
Quelle: Bitkom Research


MERCK
Tätertypen und Motive
Handlungsabsichten und Lösungsansätze
Absicht
Vorsatz
Billigende Inkaufnahme
Grobe Fahrlässigkeit
Fahrlässigkeit
(Kriminal-) Ermittlungen
Gegenmaßnahmen
Audit
Prävention
Awareness
9. Sicherheitstagung BfV & ASW | 13. Mai 2015


MERCK
Das 'Compliance Komitee'
Beispiel für einen internen Kooperationsmechanismus
Corporate Security
Internal Audit
Compliance Committee
Personal-abteilung
Group Legal
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
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. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Deutsche (Chemie-) Industrie im Fokus?
Objektive und subjektive Gefährdungskriterien
Hohe Know-how Dichte
Weltweit anerkanntes („beneidetes“) 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. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Tätertypen und Motive
[Entwurf] Erklärungsversuche Tathandeln
gesteuert
spontan
bewusst
frustriert
psychisch
ideologisch
materiell / finanziell
Politische / Ideologische Botschaft
Anschlag
Suchtverhalten
Industriespionage
Selbstverwirklichung
Rache
Wettbewerbsverzerrung
Suizid
Sabotage
Bereicherung
Aufmerksamkeit
„Job-hopping“
Leakage (‚Wiki-Leaks‘)
…
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

[redacted]

Konzernsicherheit

Sicherheitslagebild Merck Gruppe 2014 [Auszug]

[redacted]

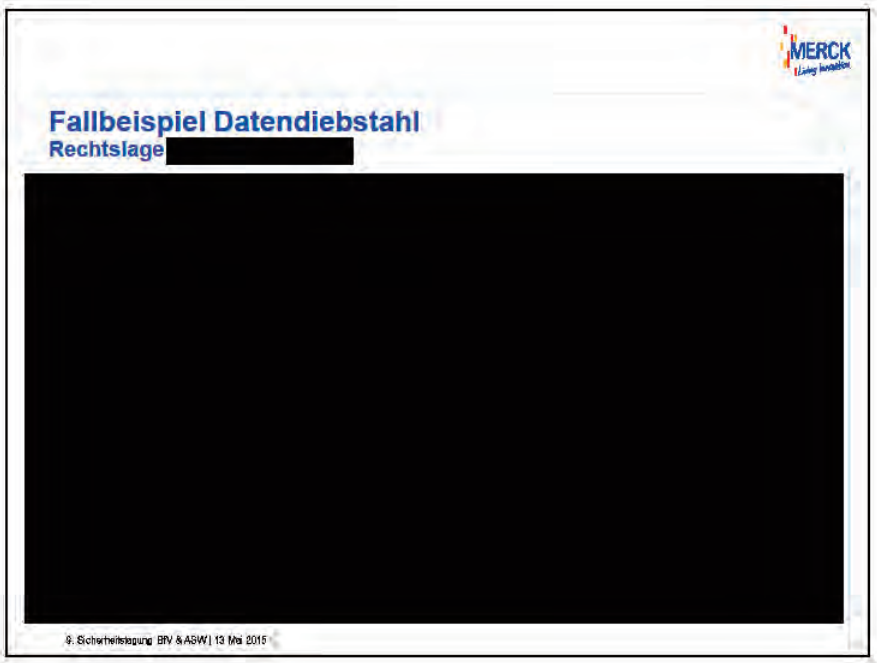
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

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 [redacted]
- [redacted]
- 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.
- [redacted]

9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Fallbeispiel Datendiebstahl
Rechtslage
[redacted]
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
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. Sicherheitstagung BfV & 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 BfV & ASW | 13 Mai 2015

Fallbeispiel 2

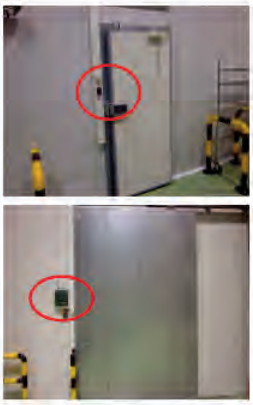
[redacted]

- 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 BfV & ASW | 13 Mai 2015

Fallbeispiel 3
Medikamentendiebstahl

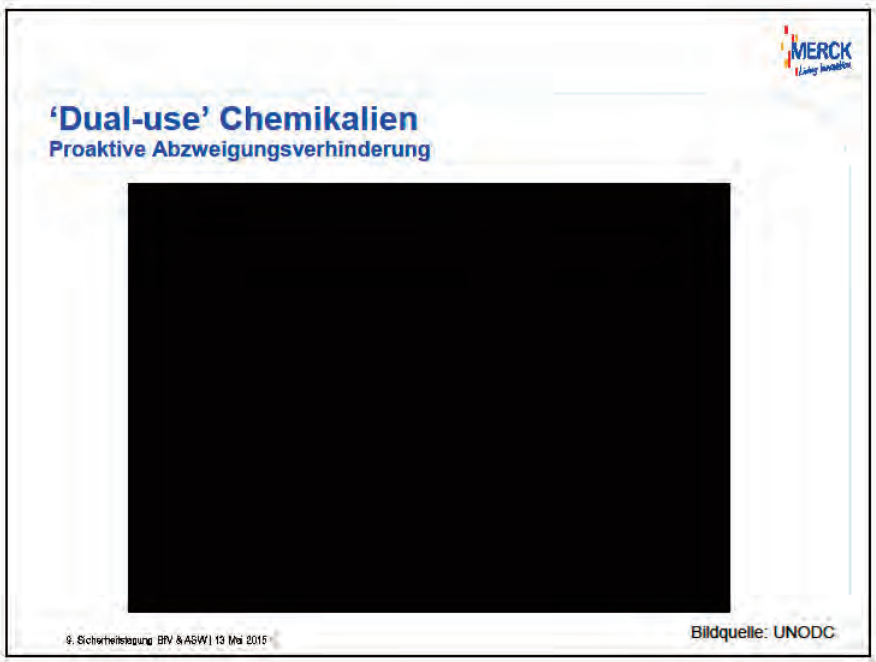
- MA hat berechtigten Zugang zu Warenlager
- MA nutzt diesen zur Begehung von Eigentumsdelikten (Diebstahl / Unterschlagung)
- Missbrauch der „Notfallprozeduren“
- Versagen der Kontrollsysteme
- Ermittlungen der lokalen Polizei
- Qualitätsaspekte für die verbliebene Rest-Charge



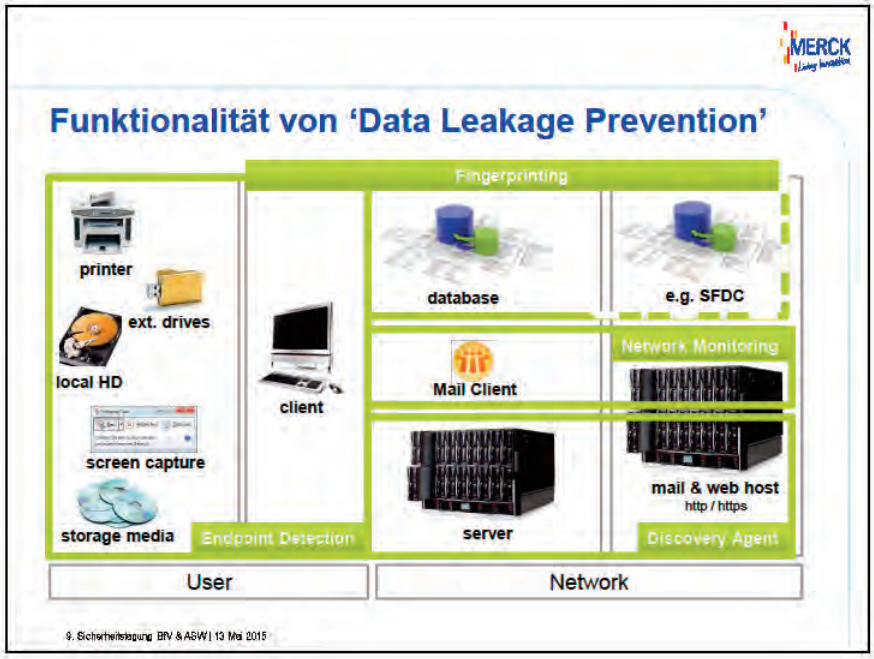
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

Corporate Security

9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
‘Dual-use’ Chemikalien
Proaktive Abzweigungsverhinderung
[redacted]
9. Sicherheitstagung BfV & ASW | 13 Mai 2015
Bildquelle: UNODC


MERCK
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
[redacted]
Quelle: Merck Mitarbeiter-Zeitung PRO, April 2014
Namen von der Redaktion geändert
PURES GOLD FÜR WETTBEWERBER
[redacted]
9. Sicherheitstagung BfV & ASW | 13 Mai 2015

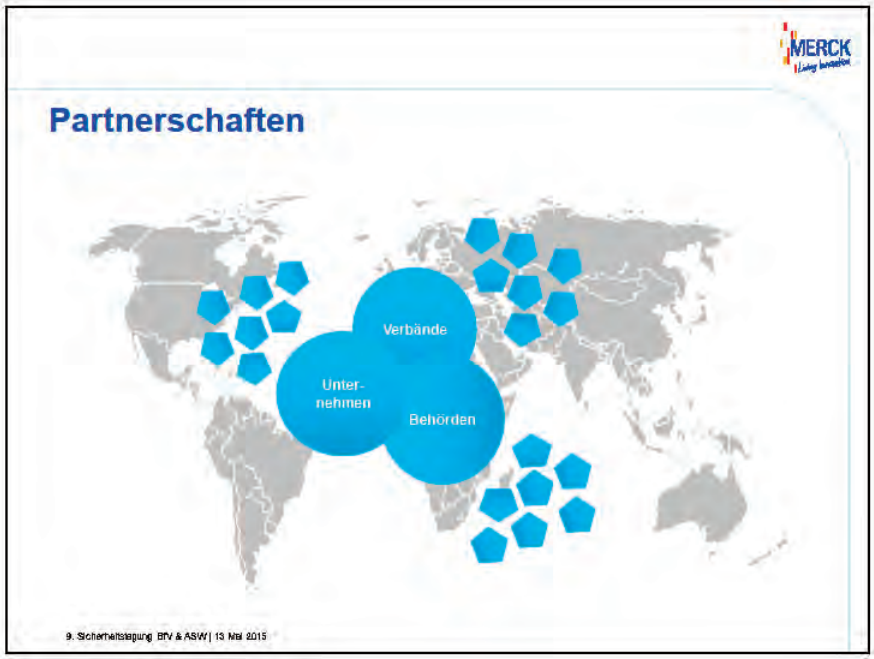

Funktionalität von ‘Data Leakage Prevention’
Fingerprinting
printer
ext. drives
local HD
screen capture
storage media
client
database
e.g. SFDC
Mail Client
Network Monitoring
server
mail & web host
http / https
Endpoint Detection
Discovery Agent
User
Network
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


Incident Management mit Hilfe von DLP
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Präventionsmöglichkeiten
Notwendigkeit eines ganzheitlichen Ansatzes
PERSONELL
"need-to-know" Prinzip / Segregieren von Aufgaben
Awareness-Trainings für betreffende MA
TECHNISCH
Technische Barrieren aufbauen (physisch / systemisch)
Detektionsmöglichkeiten erhöhen
Prozessual
HR: z. Bsp. Abgleich mit Sanktionslisten
Security: u.a."Pre-employment checks", Access-Management
IT: individualisierte Vergabe von Zugriffsrechten
INTELLIGENCE
Diskreter / offener Austausch über Partnerships
„Open-source"- Analysen
Aggregieren von Informationen durch Verbände und Behörden
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
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. Sicherheitstagung BfV & ASW | 13 Mai 2015

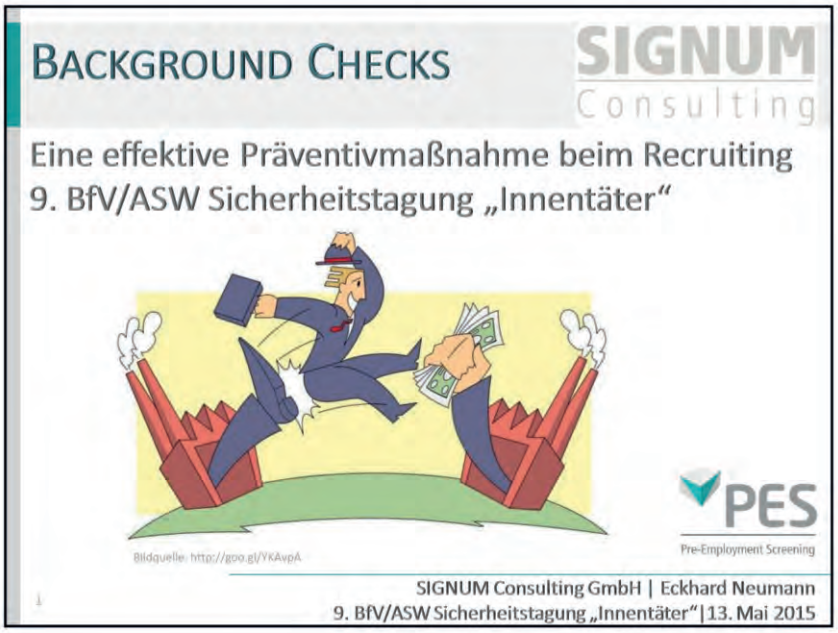

MERCK
Relevante Risiken für Merck [Auszug]
Quelle: Merck Geschäftsbericht 2014
Geschäftsbezogene Risiken
Finanzrisiken
Rechtliche Risiken
Risiken durch Produktkriminalität und Spionage
!
Risiken im Personalbereich
Risiken durch E-Crime
Umwelt- und Sicherheitsrisiken
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
Partnerschaften
Verbände
Unter-
nehmen
Behörden
9. Sicherheitstagung BfV & ASW | 13 Mai 2015


MERCK
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. Sicherheitstagung BfV & ASW | 13 Mai 2015

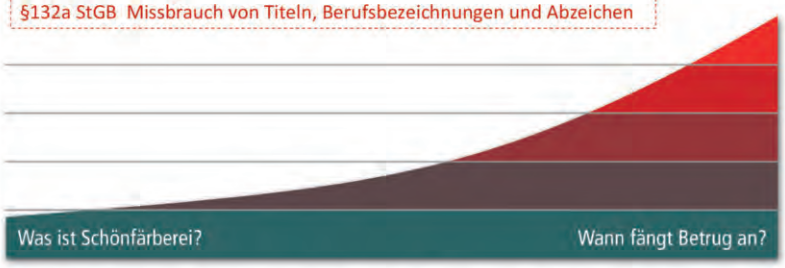
„Background Checks – eine effektive Präventivmaßnahme beim ecruiting“

Eckhard Neumann, Geschäftsführer, Signum Consulting GmbH



Von der Schönfärberei zum Betrug

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



Schokoladenseiten herausarbeiten
Aufwertung der eigenen Angaben
Schwächen kaschieren

Falschangaben z.B.
Berufsbezeichnungen
Stellenbezeichnungen
Verantwortlichkeiten

Kauf von Doktortiteln und Diplomen
Urkunden- oder Unterschriftenfälschung

3

SIGNUM Consulting

Was begünstigt Fälschung und Betrug?

Veränderungen im Bewerbungsverfahren

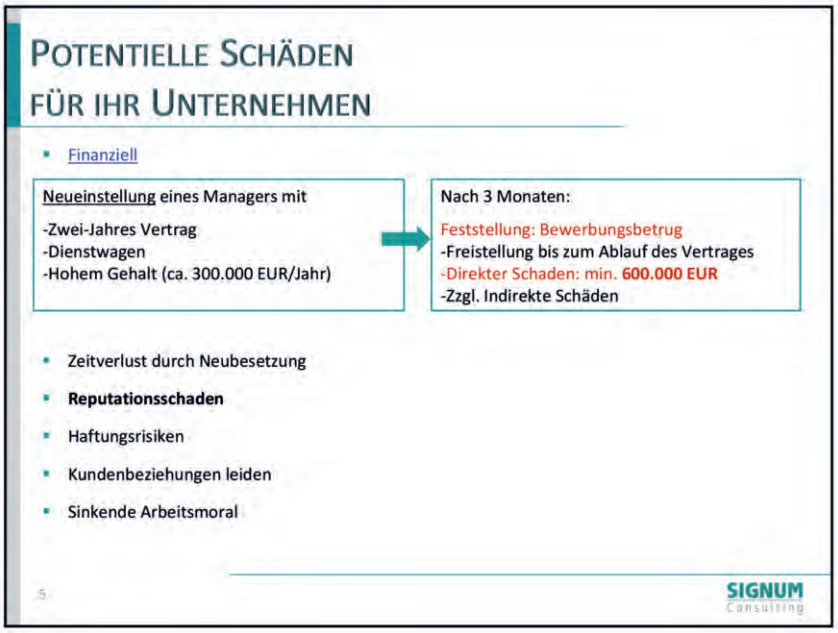
- Digitalisierung
- Internetpräsenz der Firmen und Bildungseinrichtungen
- Onlinebewerbungen
- Kandidatenpool
- Technische Möglichkeiten

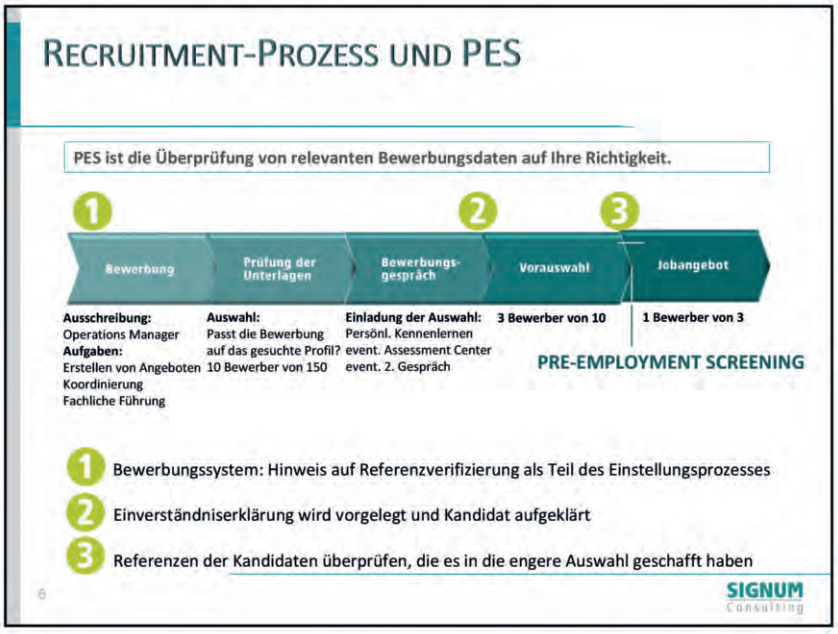
Internationalisierung des Arbeitsmarktes

- 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
SIGNUM
Consulting


RECRUITMENT-PROZESS UND PES
PES ist die Überprüfung von relevanten Bewerbungsdaten auf Ihre Richtigkeit.
1
2
3
Bewerbung
Prüfung der Unterlagen
Bewerbungs-gespräch
Vorauswahl
Jobangebot
Ausschreibung:
Operations Manager
Aufgaben:
Erstellen von Angeboten
Koordinierung
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
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
SIGNUM
Consulting

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

Frankfurter Allgemeine

Kampf gegen den Terrorismus

Der Feind in meinem Büro

Der Kampf gegen den Terrorismus macht vor Unternehmen nicht halt. Arbeitgeber wie Daimler gleichen die Daten ihrer Mitarbeiter mit Verdächtigenlisten ab. Können dabei auch Unschuldige ins Visier geraten?

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

§

EINVERSTÄNDNISERKLÄRUNG

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

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

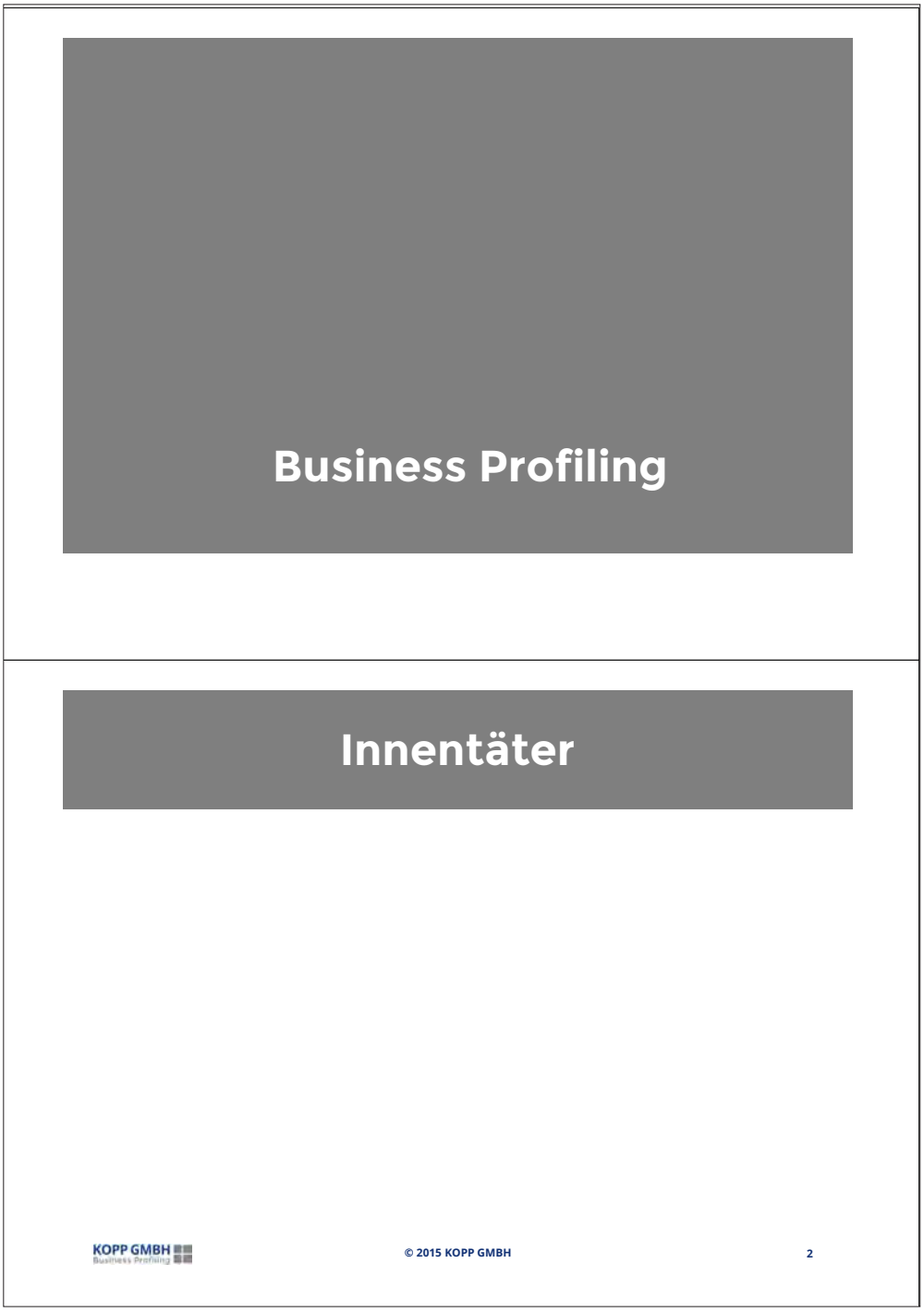
Web: www.signum-consult.com | www.pre-employment-screening.com

12

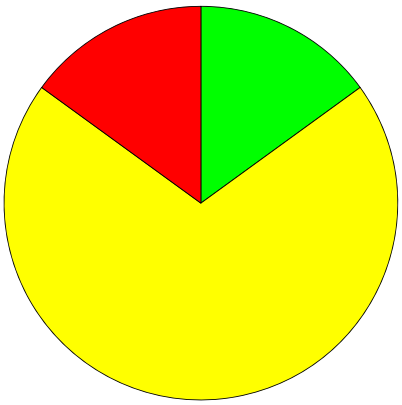
SIGNUM Consulting

„Identifizierung und Steuerung personeller Risiken mit Business Profiling“

Ralf Kopp, Geschäftsführer, KOPP GmbH



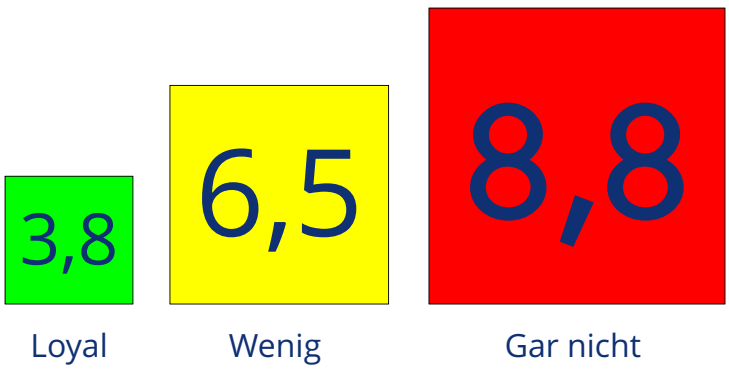
Loyalität



- 15% sehr loyal
- 70% wenig
- 15% gar nicht

KOPP GMBH Business Profiling © 2015 KOPP GMBH Quelle: Gallup 3

Fehltage



KOPP GMBH Business Profiling © 2015 KOPP GMBH Quelle: Gallup 4

Innentäter

sind immer illoyal

KOPP GMBH Business Profiling

5

Loyalität basiert auf

- Menschenkenntnis
- Kommunikation
- Führung

KOPP GMBH Business Profiling

6

Zusammenhang

Mangelhafte Steuerungsfähigkeiten

↓

Wenig Loyalität

↓

Viele Innentäter

KOPP GMBH Business Profiling

7

Die Unternehmen

produzieren ihre Innentäter selbst

KOPP GMBH Business Profiling

8

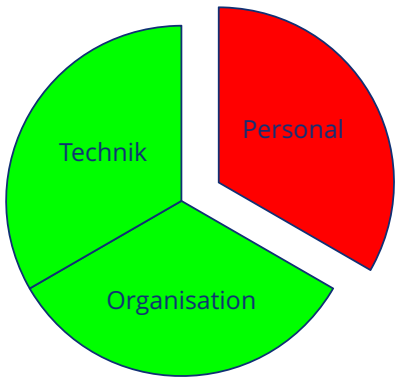
Ist Loyalität

in Ihrem Unternehmen ein Thema?

KOPP GMBH Business Profiling

9

TOP



KOPP GMBH Business Profiling

10

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

KOPP GMBH Business Profiling

Quelle: Mercer

11

Respectare

genau hinsehen

KOPP GMBH Business Profiling

12

Neurowissenschaften

„Keiner kann anders, als er ist“

Prof. Wolf Singer

KOPP GMBH Business Profiling

13

Eigenschaften sind Hardware

KOPP GMBH Business Profiling

14

Sigmund Freud

„Unsere Persönlichkeit

dringt uns jeden Tag aus allen Poren“

KOPP GMBH Business Profiling

15

Criminal Profiling

Empirische Täterprofile

KOPP GMBH Business Profiling

16

Systematischer Prozess

der subjektive Beurteilungen

weitgehend ausschaltet

KOPP GMBH Business Profiling

17

Objektive Merkmale

- Lebenslauf
- Beobachtungen
- Interviews
- Internetrecherche

KOPP GMBH Business Profiling

18

Ausbildung

Jede Entscheidung sagt etwas aus

KOPP GMBH Business Profiling

19

Kommunikationsebene

- Sachebene
- Beziehungsebene
- Appellebene
- Selbstkundgabeebene

KOPP GMBH Business Profiling

20

Quantitative Sprachanalyse

Worte

↓

Denkmuster

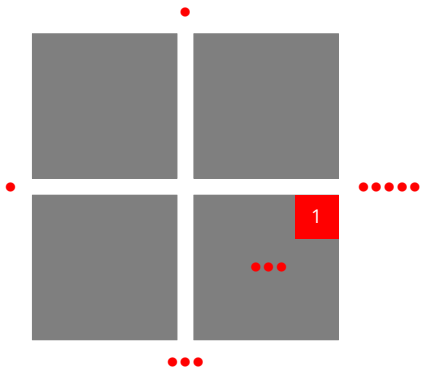
↓

Persönlichkeitsstruktur

KOPP GMBH Business Profiling

21

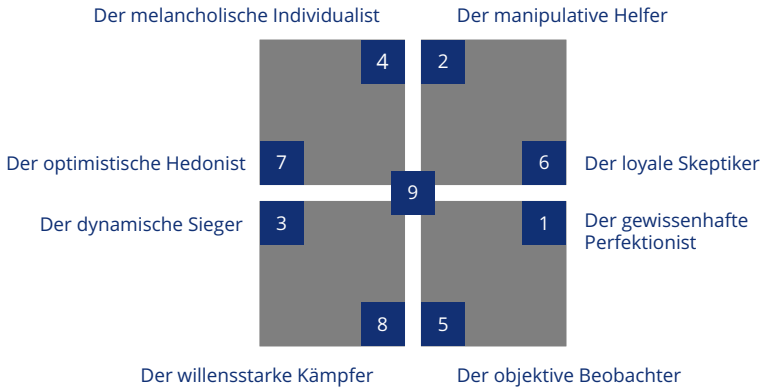
Profiling-Kreuz



KOPP GMBH Business Profiling

22

9 Typen



KOPP GMBH Business Profiling

23

Eigenschaften

- Loyalität
- Integrität
- Regeltreue
- Risikoneigung

KOPP GMBH Business Profiling

24

Mehr Eigenschaften

- Verhalten in Konflikten
- Verhalten in Verhandlungen
- Trigger

KOPP GMBH Business Profiling

25

Typologien und Strukturmodelle

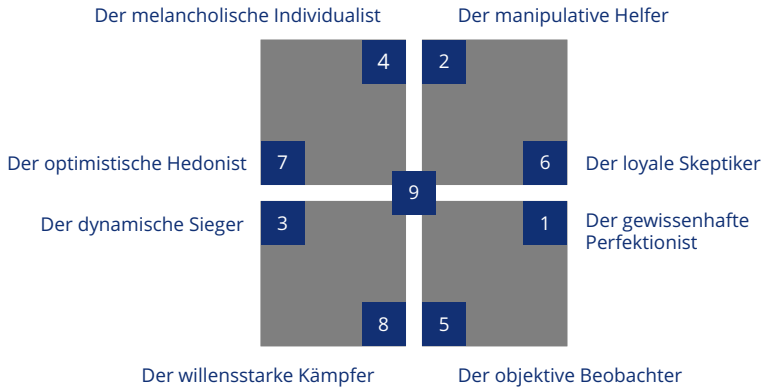
Jung	Big Five	MBTI/Keirsey	DISG
Fromm			LIFO
Adler			TMS
Weber			BIP
Horney			Reiss/16PF
Ekman			HBDI
Eysenck			SASB
Murray	von Thun	Maccoby	STAR/PSI

Riemann

KOPP GMBH Business Profiling

26

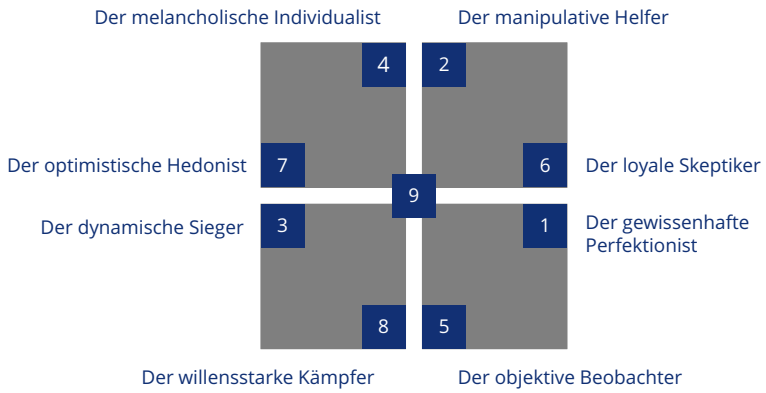
Beispiele Berufe



KOPP GMBH Business Profiling

27

Beispiele Personen



KOPP GMBH Business Profiling

28

Unterschiede 1 und 3

Eigenschaft	Typ 1	Typ 3
Loyalität	★★★☆☆	★☆☆☆☆
Integrität	★★★★★	★☆☆☆☆
Regeltreue	★★★★★	★☆☆☆☆
Risikoneigung	★☆☆☆☆	★★★★★

KOPP GMBH Business Profiling

29

Spezielle Situationen

Dilemma der 1

KOPP GMBH Business Profiling

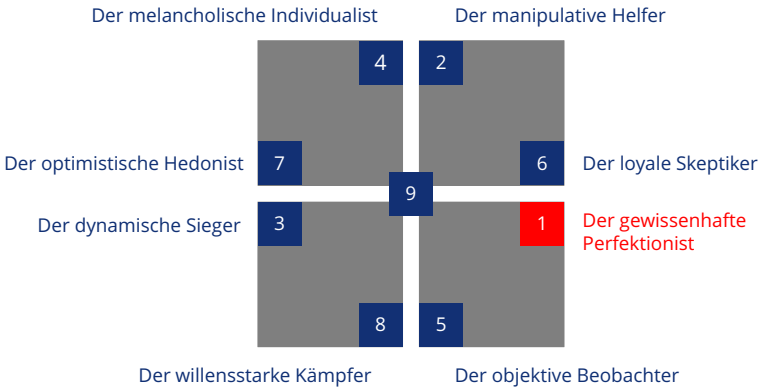
30

Unterschiede 1 und 6

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

KOPP GMBH Business Profiling © 2015 KOPP GMBH 31

Snowden



KOPP GMBH Business Profiling © 2015 KOPP GMBH 32

IT-Admin

Kündigung

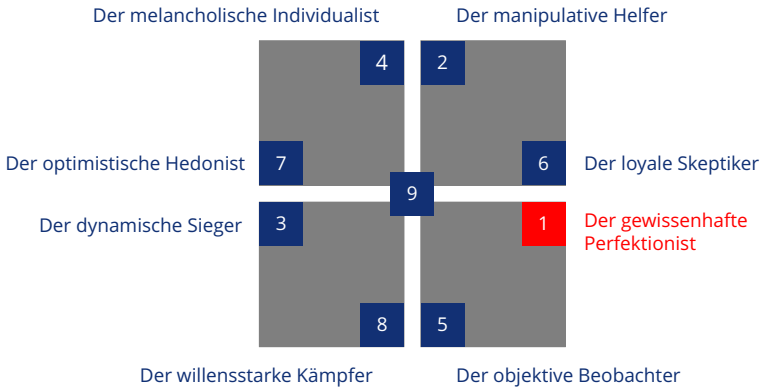
↓

Illegale Datenzugriffe

KOPP GMBH Business Profiling

33

IT-Admin



KOPP GMBH Business Profiling

34

Gleichwertigkeit

Alle Strukturen sind gleichwertig.

Nur anders.

KOPP GMBH Business Profiling

35

Ähnlichkeitsfalle

Wir mögen die Menschen,

die so sind, wie wir selbst sind

KOPP GMBH Business Profiling

36

Psychopathen

im medizinischen Sinne

nach Prof. Robert Hare

KOPP GMBH Business Profiling

37

Hare-Skala

0-40

KOPP GMBH Business Profiling

38

Psychologisches Inventar

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

KOPP GMBH Business Profiling

39

Häufigkeit

5%

KOPP GMBH Business Profiling

40

Funktionale Psychopathen

Top-Performer

KOPP GMBH Business Profiling

41

Dysfunktionale Psychopathen

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

KOPP GMBH Business Profiling

42

Champions League

der Innentäter

KOPP GMBH Business Profiling

43

1. Bewusstsein entwickeln

Persönlichkeitsstrukturen

Menschenkenntnis Kommunikation

Führung Respekt Loyalität

Innentäter

KOPP GMBH Business Profiling

44

2. Zusammenhang

sichtbar machen

KOPP GMBH Business Profiling

45

3. Risiken identifizieren

- Illoyale Mitarbeiter
- Loyale Mitarbeiter in Konflikten
- Dysfunktionale Psychopathen

KOPP GMBH Business Profiling

46

4. Mitarbeiter in Konflikten

unterstützen

KOPP GMBH Business Profiling

47

5. Führungskräfte trainieren

- Menschenkenntnis
- Kommunikation
- Führung

KOPP GMBH Business Profiling

48

6. Psychopathen

Entfernen Sie

dysfunktionale Psychopathen

KOPP GMBH Business Profiling

49

Wirtschaftlichkeit

Investition in

- Menschenkenntnis
- Kommunikation
- Führung

Schäden durch

- Straftaten
- Andere schädigende Handlungen

KOPP GMBH Business Profiling

50

Trainings in Business Profiling

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

KOPP GMBH Business Profiling

51

Vielen Dank!

www.koppgmbh.de

„Wirtschaftsschutzgrundhandbuch – Vorhang auf für die ersten Bausteine“

Prof. Timo Kob, Vorstandsmitglied, ASW Bundesverband

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!

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 5

Die Projektpartner

HISOLUTIONS

ASW Bundesverband

ASW Bundesverband

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

HISOLUTIONS

- Beratungsspezialist für Informations-sicherheit 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 WISPER 22. 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

Forschungsprojekt WISPER 22. Juni 2015 – Folie 7

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

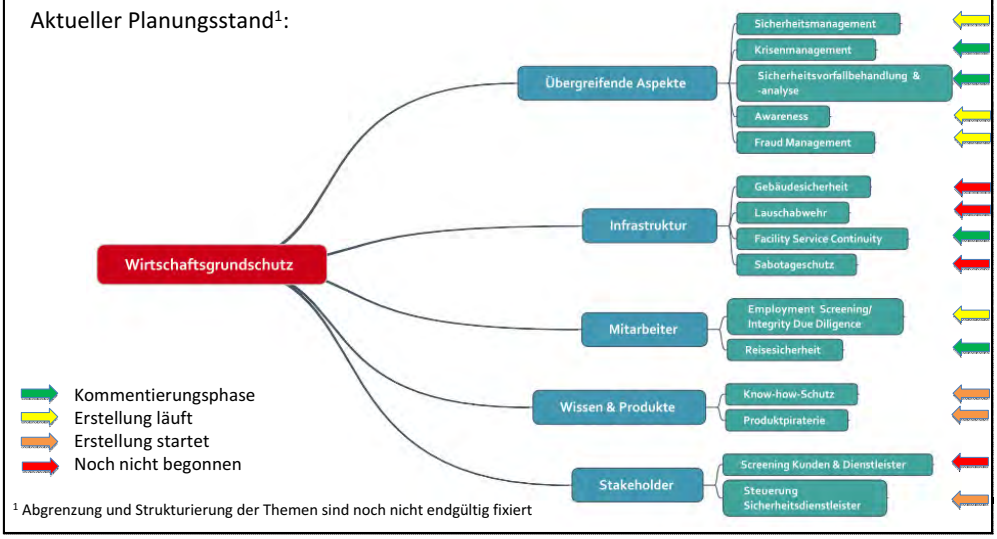
Bausteine fassen konkrete Maßnahmen zu einem Themenkomplex zusammen. Die Maßnahmen werden nach ihrer Bedeutung kategorisiert/priorisiert.

Ebene 3 – Vertiefungsdokumente

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

Präsentationstitel in Kopf- Fußzeile 22. Juni 2015 – Folie 8

Aktueller Planungsstand[1]:



[1] Abgrenzung und Strukturierung der Themen sind noch nicht endgültig fixiert

Beispielbaustein Krisenmanagement

HISOLUTIONS ASW Bundesverband

Präsentationstitel in Kopf Fußzeile 22. Juni 2015 – Folie 10

Das Wichtigste auf einen Blick (Themenübersicht)

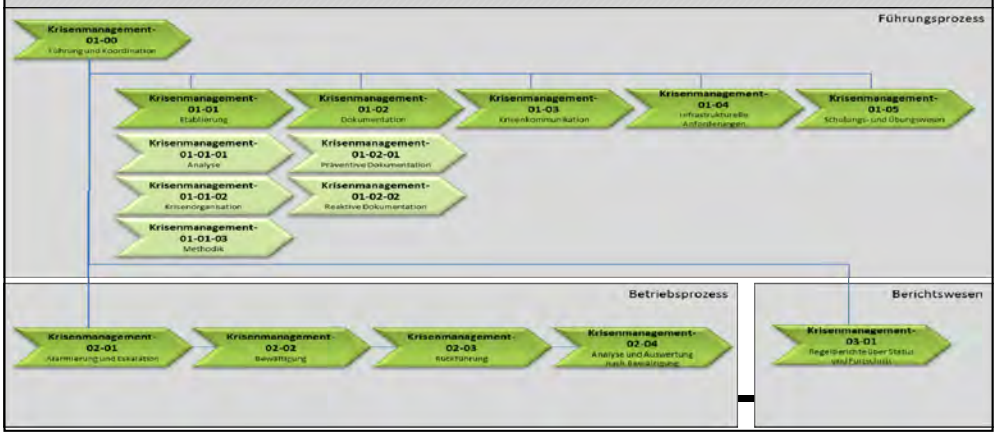
HISOLUTIONS ASW Bundesverband

Analyse	Krisenorganisation	Dokumentation	Infrastruktur
•Identifikation von Bedrohungen und Gefährdungen mit besonderem Krisenpotential	•Organisationsstruktur •Aufbau Krisenstab •Kompetenzen, Verantwortlichkeiten und Aufgaben	•Leitlinie, Rahmenwerk •Krisenhandbuch •Alarmierungskonzept •Geschäftsordnung •Krisenplan •Alarmierungsplan •Checklisten, Rollenkarten •Vorlagen und Werkzeuge	•Krisenstabsraum
Methodik Krisenstab	**Krisenkommunikation**	**Schulungswesen**	**Übungswesen**
•Lagebeurteilung/-bearbeitung •Entscheidungsfindung •Dokumentation, Protokollierung •Visualisierung •Schichtwechsel und Lageübergabe	•Identifikation und Analyse der Interessengruppen •Rollen und Definition der Kompetenzen, Verantwortlichkeiten und Aufgaben •Medienbeobachtung •Kommunikationsmittel und -materialien	•Identifikation des Schulungsbedarfs •Erstellung von Schulungskonzepten •Erstellung eines Schulungsregelwerkes •Durchführung von Schulungen	•Entwicklung eines Übungsprogramms •Standardisierung des Übungszyklus •Übungsrollen •Erstellung der Übungsdokumentation

– Folie

Ablaufdiagramm des Themenfelds

HISOLUTIONS ASW Bundesverband



M3 Aufbau eines Krisenstabs (A)

HISOLUTIONS ASW Bundesverband

Inhalt	Kurzbeschreibung
Charakter	▪ besondere Aufbauorganisation mit besonderen Befugnissen ▪ zentrales Krisenmanagementorgan mit allen erforderlichen abteilungsübergreifenden Kompetenzen
Aufgaben	▪ Erstellen und Bewerten des Lagebilds ▪ Entwickeln und Bewerten von Handlungsoptionen ▪ Steuern der Bewältigungsmaßnahmen ▪ Koordinieren der Zusammenarbeit mit Dritten ▪ Organisieren der Stabsarbeit ▪ Organisieren der internen und externen Krisenkommunikation
Besetzung	▪ Kernteam ▪ Erweiterter Krisenstab ▪ Unterstützende Funktionen

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

M10 Erstellen eines Krisenplans (A)

HISOLUTIONS ASW Bundesverband

Inhalt	Kurzbeschreibung
Charakter	▪ reaktives und einsatzorientiertes Dokument ▪ enthält die wichtigsten Informationen zur systematischen Bewältigung von Krisenereignissen
Themen	▪ Erstmaßnahmen ▪ Lagebearbeitung ▪ Führung ▪ Deeskalation und Rückführung
Weitere Informationen	▪ Agenda für das erste Zusammentreffen des Krisenstabs ▪ Kompetenzen und Verantwortlichkeiten ▪ Kontaktinformationen ▪ Verfahren zur methodischen und Szenario-spezifischen Arbeit ▪ Vorlagen für Krisenstabsprotokoll, Lagebericht, Visualisierung

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

M22 Erstellen eines Krisenkommunikationsplans (A)

HISOLUTIONS ASW Bundesverband

Inhalt	Kurzbeschreibung
Charakter	▪ vorrangig reaktives Dokument ▪ beschreibt die Kontrolle und Steuerung der Informationsflüsse
Themen	▪ Analyse der Interessengruppe ▪ Medienbeobachtung und -management ▪ Entwicklung der Krisenkommunikationsstrategie ▪ Interne und externe Kommunikation
Weitere Informationen	▪ Grundlagen Krisenkommunikation und Kommunikationsregeln ▪ Kommunikationsmittel und -materialien ▪ Liste der Interessensgruppen (Stakeholder-Matrix) ▪ Vorbereitete Inhalte (z.B. Mustertexte, FAQ) ▪ Kontaktliste zu Medien/Experten

Präsentationstitel in Kopf- Fußzeile 22. Juni 2015 — Folie 15

Übersicht der Maßnahmen des Bausteins

HISOLUTIONS ASW Bundesverband

A – Erstmaßnahmen

M1 Identifikation von Bedrohungen und Gefährdungen mit besonderem Krisenpotential
M3 Aufbau eines Krisenbewältigungsgremiums
M4 Definition der Kompetenzen, Verantwortlichkeiten und Aufgaben
M10 Erstellen eines Krisenplans
M15 Bereitstellen geeigneter Räumlichkeiten für den Krisenstab
M17 Definieren der Verfahrensweisen für die Lagebeurteilung und -bearbeitung sowie Entscheidungsfindung
M18 Definieren der Verfahrensweisen für die Dokumentation
M22 Erstellung eines Krisenkommunikationsplans
M23 Festlegen der Rollen und Definition der Kompetenzen, Verantwortlichkeiten und Aufgaben der Krisenkommunikation
M25 Definition der Kommunikationsmittel und -materialien
M27 Identifizieren des Schulungsbedarfs
M28 Erstellen eines Schulungskonzepts
M30 Durchführen von Schulungen
M34 Identifikation und Erstellung der erforderlichen Übungsdokumentation

B – Basismaßnahmen

Maßnahmen A
+
M2 Entwicklung einer geeigneten Organisationsstruktur
M5 Erstellen einer Leitlinie und Übernahme der Gesamtverantwortung
M6 Erstellen eines Rahmenwerks
M8 Erstellen eines Alarmierungskonzepts
M11 Erstellen eines Alarmierungsplans
M12 Entwickeln von Szenario-spezifischen Checklisten
M19 Definieren der Verfahrensweisen für die Visualisierung
M21 Identifikation und Analyse der Interessengruppen
M24 Festlegen eines Verfahren für die Medienbeobachtung
M26 Aufbau einer Darksite / Shadowsite
M29 Erstellen des erforderlichen Schulungsregelwerks
M31 Entwicklung eines Übungsprogramms
M32 Definition eines standardisierten Übungszyklus
M33 Definition der erforderlichen Übungsrollen

C – erweiterte Maßnahmen

Maßnahmen A und B
+
M7 Erstellen eines Krisenhandbuchs
M9 Erstellen einer Geschäftsordnung für den Krisenstab
M13 Erstellen von Rollenkarten
M14 Bereitstellen aller notwendigen Vorlagen und Werkzeuge
M16 Definieren der Verfahrensweisen zur Erarbeitung der Krisenmanagementstrategie
M20 Definieren der Verfahrensweisen für den Schichtwechsel und die Lageübergabe


HISOLUTIONS
ASW
Bundesverband
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
+49 (0) 30 200 77 200
ASW
Bundesverband
Forschungsprojekt WISPER
22. Juni 2015 – Folie 17

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

Frank Eckhardt, Leiter Lauschabwehr, Deutsche Telekom AG

ERLEBEN, WAS VERBINDET.

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 Lauschabwehrüberprüfung (Sweep):

- ✓ Funktechnische Untersuchung
- ✓ Glastransmissionsmessung
- ✓ Halbleiterdetektion
- ✓ Leitungsuntersuchung
- ✓ Röntgenuntersuchung
- ✓ Visuelle Untersuchung
- ✓ Wärmebildanalyse

Bewahren Sie sich vor Informationsverlusten und sichern Sie Ihr Business!

ERLEBEN, WAS VERBINDET. ASW und BfV – „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

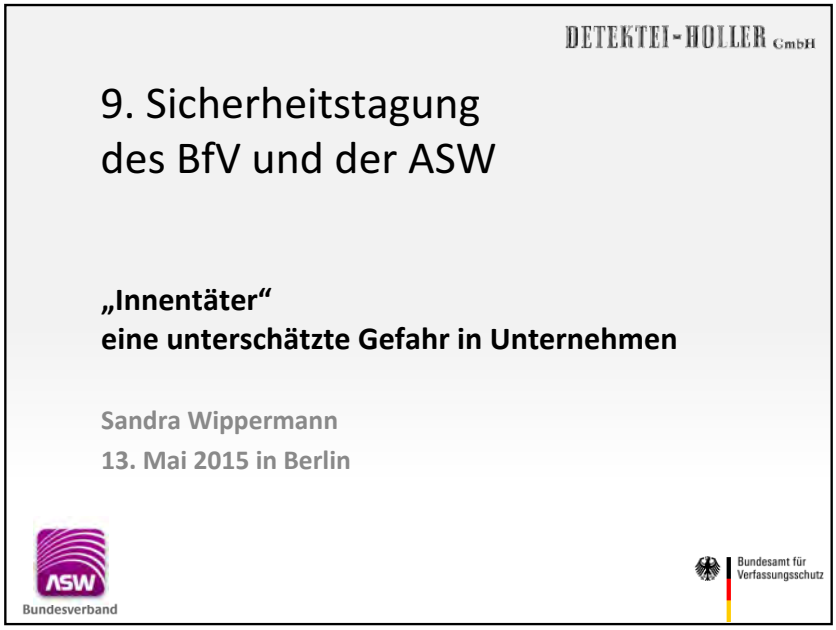
untersuchtes Objekt

ERLEBEN, WAS VERBINDET. ASW und BfV – „Innentäter“ eine unterschätzte Gefahr 13.05.2015 Seite 6


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.

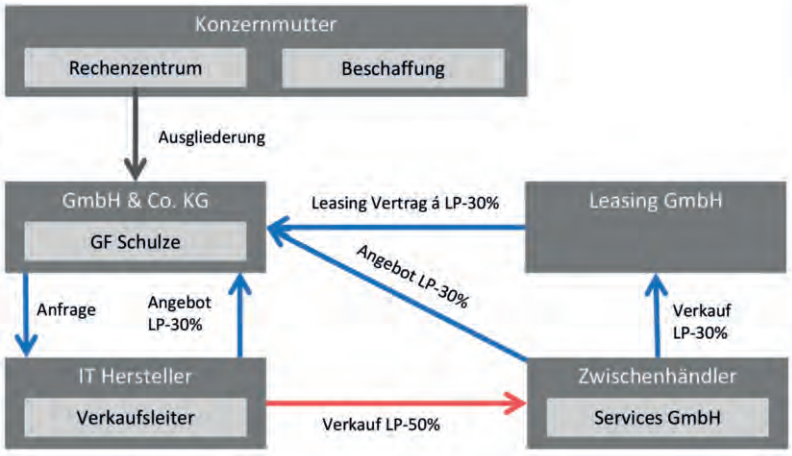
„Detektion aus der Praxis – Beispiele national/international agierender Unternehmen“

Sandra Wippermann, Gesellschafterin, Detektei – Holler GmbH



DETEKTEI-HOLLER GmbH

Maverick Buying



DETEKTEI-HOLLER GmbH

Maßnahmen nach dem Schadensfall

- Erweiterte Funktionstrennung
- Ausschreibungen und Verhandlungen nur über den Einkauf
- Zusätzliche Genehmigungsstufen für Bestellvorgänge
- Zusätzliche Inventarkontrollprozesse
- Bestandsdatei für Leasingwirtschaftsgüter
- Schulung mit Fall-Beispielen für Bedarfsträger und Einkäufer

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

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

Gestaltung und Druck
Bundesamt für Verfassungsschutz
Print- und Mediencenter

Bildnachweis
© FotolEdhar - Fotolia.com
© Mike Minehan
© BfV/ASW

Stand
Juli 2015

Wirtschaftsschutz
ist
Teamwork