Bundesamt für
Verfassungsschutz

ASW
Zentralorganisation der Wirtschaft

Proaktiver Wirtschaftsschutz: Prävention durch Information

8. Sicherheitstagung des BfV und der ASW am 03. Juli 2014 in Berlin

Tagungsband

„Proaktiver Wirtschaftsschutz: Prävention durch Information“

8. Sicherheitstagung des BfV und der ASW am 3. Juli 2014 in Berlin

Tagungsband

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
IT 21.2 Print- und Mediengestaltung

Bildnachweis
BfV

Stand
September 2014

Inhaltsverzeichnis

8. Sicherheitstagung des BfV und der ASW am 3. Juli 2014 in Berlin

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

Unter dem Motto „Proaktiver Wirtschaftsschutz: Prävention durch Information“ fand am 3. Juli die 8. BfV/ASW-Sicherheitstagung in Berlin statt. Etwa 100 Experten aus Sicherheitsbehörden und Wirtschaft erörterten Risiken, Abwehrmaßnahmen und Sensibilisierungsstrategien für die deutsche Wirtschaft. Übereinstimmend wurde ein Nachholbedarf beim Sicherheitsbewusstsein, insbesondere in mittelständischen Unternehmen, festgestellt.

Wirtschaftsschutz ist wichtiger, denn je. Wirtschaftsspionage ist tägliche Realität. Die vielfältigen Herausforderungen im Wirtschaftsschutz erfordern ein Zusammenwirken von Staat und Wirtschaft. Die Kooperation zwischen BfV und ASW ist hierbei ein wichtiger Baustein.

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 8ten BfV/ASW Tagung zum Thema

„Wirtschaftsschutz: Prävention durch Information“ begrüßen zu dürfen.

Wer sich mit dem Thema befasst, wird die aktuelle Dynamik der Bedrohungen schnell erkenne. Die letzten 12 Monate haben uns die Bedeutung noch einmal deutlich vor Augen geführt. So war das Thema doch im Zusammenhang mit den Snowden-Enthüllungen und der daraus entbrannten politischen Diskussion ein Dauerbrenner in den Leitmedien. Schwierig ist, dass unsere Gesellschaft und Unternehmen zwar immer mehr für das Bedrohungspotenzial sensibilisiert sind, aber die eigene mögliche Betroffenheit immer noch unterschätzt wird.

Dabei sind die zunehmenden Risiken, insbesondere durch Wirtschaftskriminalität und Spionage, deutlich spürbar und fordern Politik, Wirtschaft und Gesellschaft in immer stärkerem Maße zum Handeln. Diese gesellschaftliche Bedeutung hat auch die Bundesregierung erkannt und Wirtschaftsschutz als ein Leitthema zum ersten Mal in einem Koalitionsvertrag mit aufgenommen. Das – finde ich übrigens – ist ein bedeutender Schritt und ein großer Erfolg für unser Engagement dem Thema mehr Gewicht zu verleihen!

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 in dem wir uns

1) als aktiver Partner in der politischen Gesetzgebung positionieren,
2) als „das“ 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. Und das tun wir bereits heute ganz konkret im Steuerungskreis Wirtschaftsschutz, wo wir gemeinsam an einer nationalen Wirtschaftsschutzstrategie 2015 arbeiten. Die derzeitige Ausgestaltung dieser Strategie entwickelt sich entlang 5 identifizierter Handlungsfelder, die da wären:

1) Informationsaustausch: Schaffung einer Sicherheitsplattform mit den zentralen Ansprechpartnern von Wirtschaft Staat/Sicherheitsbehörden.
2) Sicherheitsprozesse/-maßnahmen: Ausbau der Vertrauenskultur zwischen Wirtschaft und Staat. Auf Erreichtem weitermachen. Hier sind in erster Linie unsere Partnerschaften mit den Sicherheitsbehörden. Da die Tagung mit dem BfV bereits die 8. Tagung ist, können wir ja schon von einer Tradition sprechen.
3) Sensibilisierung/Prävention: Sensibilisierung von Wirtschaft und Behörden für Risiken und Belange des Wirtschaftsschutzes. Hier stellen wir uns eine gemeinsame Kampagne von Staat und Wirtschaft vor.
4) Ausbildung/Qualifizierung: Neue Qualität eines umfassenden Sicherheitsmanagements. AK Aus- und Weiterbildung.
5) Zertifizierung/Normierung/Standards: Sicherheit auf hohem Niveau! Technik, Prozesse, Menschen (Qualifizierung)

Hierzu werden in den jeweiligen Expertengruppen bestehend aus Vertretern von Wirtschaft, Ministerien & Sicherheitsbehörden Maßnahmen und Lösungsansätze erarbeitet. Ich freue mich, dass auch hier die ASW und ihre Mitglieder ihren gestalterischen Beitrag leisten werden.

Nun aber zum heutigen Tag! Dass Sie so zahlreich erschienen sind, zeigt mir, dass wir hier die richtigen Themen ansprechen und es freut mich Ihnen auch dieses Jahr eine abwechslungsreiche Agenda mit hervorragenden Referenten präsentieren zu können.

Das Leitthema unserer heutigen Agenda ist: Prävention durch Information, denn nur wenn man sich der aktuellen Bedrohung bewusst ist, kann man entsprechende Gegenmaßnahmen ergreifen. Und damit starten wir gleich mit einer sicherlich bereichernden Keynote unseres BfV Präsidenten zur aktuellen Situation.

Und da Globalisierung und virtuelle Vernetzung ihr Übriges dazutun, den Schutz zu einer hoch komplexen Herausforderung zu machen, finde ich es

gut, dass wir Ihnen auch in diesem Jahr eine internationale Perspektive zum Thema bieten können. Unsere niederländischen Nachbarn sind nämlich ein wichtiger Partner in Sachen Wirtschaftsschutz. Herr Marten Hidskes herzlich willkommen, wir sind gespannt auf Ihre Ausführungen.

Im weiteren Verlauf warten dann auf uns mehr praxisorientierte Themen bezogen auf elektronische Angriffe und die unterschätzte Gefahr der Industriespionage, die uns alle direkt betreffen. Fred Maro, ein Experte zu Social Engineering, blickt beim Thema Industriespionage vor allem auf den Faktor Mensch. Herr Jadran Mesic geht auf die technische Seite ein. Gerade in diesem Zusammenhang darf die präventive Bedeutung von geschulten Mitarbeitern nicht unterschätzt werden. Dazu wird mein Vorstandskollege Manfred Jilg uns hier ein paar Einblicke in die Möglichkeiten und Arbeit des Kompetenzcenters Aus- und Weiterbildung gewähren.

Ein besonderes Highlight ist für mich dann auch immer die Abschlussdiskussion mit allen Referenten des Tages. Ihre Möglichkeiten offene Fragen zu klären und den Experten nochmals auf den Zahn zu fühlen!

Ich bin sicher, auch in diesem Jahr wird unsere „traditionelle“ und bereits 8. 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 und der Power Unternehmensgruppe bedanken, die dazu beigetragen haben, das heutige Setting in diesem Umfang möglich zu machen.

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

Begrüßung und Keynote durch den Präsidenten des BfV, Dr. Hans-Georg Maaßen

- Es gilt das gesprochene Wort! -

Meine sehr verehrten Damen und Herren, lieber Herr Wagner,
ich freue mich sehr, Sie anlässlich der 8. BfV/ASW-Sicherheitstagung begrüßen zu können.

Wirtschaftsschutz und Wirtschaftsspionage sind für den Verfassungsschutz schon seit einigen Jahren von Bedeutung.

Vor nicht allzu langer Zeit hatte man mit diesem Thema allerdings Mühe, Gehör zu finden: auch und gerade bei der Wirtschaft selbst. Das ist heute anders, die Bedrohungslage hat sich erheblich verschärft.

Deutschland steht auf Platz zwei im Export-Ranking. Ein Erfolg, der maßgeblich auf der Wettbewerbsfähigkeit und Innovationskraft seiner Unternehmen beruht, nicht zuletzt auch der mittelständischen Firmen. Es ist ein gemeinsames Interesse von Staat und Wirtschaft, den Standortvorteil zu verteidigen – auch und gerade vor dem Hintergrund eines harten internationalen Wettbewerbs und beschleunigter Innovationszyklen.

Die herausragende Stellung der deutschen Wirtschaft und ihrer Unternehmen weckt Begehrlichkeiten - bei fremden Nachrichtendiensten ebenso wie bei konkurrierenden Unternehmen. Wirtschaftsspionage und Konkurrenzausspähung richten sich verstärkt gegen technologieorientierte und innovative deutsche Unternehmen.

In regelmäßigen Abständen entnehmen wir der Presse Meldungen über neue Datenskandale und müssen feststellen: Die Integrität informationstechnischer Systeme und die Vertraulichkeit der dort vorhandenen Daten sind zu entscheidenden Zukunftsfragen geworden.

Spionage ist Realität – auch und gerade in einer globalisierten Welt. Sie betrifft nicht nur den politischen und militärischen Raum, sondern richtet sich auch gegen die Wirtschaft. Das zeigen seit Jahren auch Studien und Umfragen zur Unternehmenssicherheit.

Dies wird u.a. auch durch die ASW-Sicherheitsenquete 2013 deutlich: 45% der befragten Unternehmensvertreter geben an, Opfer von Cybercrime oder Ausspähung gewesen zu sein. Noch deutlicher werden 77% der Befragten: Sie gehen davon aus, dass die Gesamtgefährdungslage für die deutsche Wirtschaft künftig noch zunehmen wird.

Worin liegt diese Entwicklung begründet?

Während Global Player oder große Unternehmen zumeist über eine Sicherheitsabteilung verfügen mit gut ausgebildetem Personal und entspre-

chenden Sicherheitsstrukturen, ist es um technologieorientierte und innovative mittelständische Unternehmen schlechter bestellt. Sie verfügen nur selten über ein Informationsschutzkonzept. Vielfach sind sich Vorstände und Geschäftsführer der Risiken ungewollten Know-how-Verlustes nicht bewusst, zumindest nicht in dem Maße, wie dies notwendig wäre.

Die Ergebnisse der ASW-Sicherheitsenquete 2013 überraschen daher in diesem Zusammenhang nicht:

Weniger als die Hälfte der befragten Unternehmen besitzen überhaupt ein Sicherheitsmanagement mit klaren Regeln für den Informationsschutz. Nur jedes fünfte Unternehmen hat seine „Kronjuwelen“, also das schützenswerte Know-how im Unternehmen, definiert.

Lassen Sie mich zum Abschluss einige Aspekte zum „Proaktiven Wirtschaftsschutz“ vortragen.

Wirtschaftsschutz und die Abwehr digitaler Spionage sind zentrale Themen der Sicherheitsbehörden.

Das Handeln einzelner Akteure wird nicht ausreichen, um globale Spionageangriffe abzuwehren.

Wir als BfV können der deutschen Wirtschaft helfen, solche Risiken realistisch einzuschätzen, konkrete Gefahren frühzeitig zu erkennen und effektive Abwehrstrategien zu entwickeln. Die bisher schon vorhandenen Kontakte und gute Erfahrungen bei der Sensibilisierung von deutschen Unternehmen müssen ausgebaut und verstetigt werden.

Ein wichtiger Meilenstein auf dem Weg zu einer nationalen Wirtschaftsschutzstrategie ist die am 28. August 2013 durch den Bundesminister des Innern sowie den Präsidenten des Bundesverbandes der Deutschen Industrie und des Deutschen Industrie- und Handelskammertages unterzeichneten Erklärung „Wirtschaftsschutz in Deutschland 2015 – Vertrauen, Information, Prävention“.

Die mit dieser Erklärung verbundenen Absichten und Handlungsziele stellen die bisherigen Aktivitäten auf eine neue und zukunftsweisende Stufe.

Es gilt nunmehr die bisherigen Aktivitäten und Erfahrungen sowie die angestoßenen Initiativen von Staat und Wirtschaft noch stärker zu vernetzen, intensiver abzustimmen und mit dem jeweiligen Know-how und den vorhandenen Möglichkeiten noch effektiver zu gestalten, um auch Synergie-Effekte zu erzielen.

Wir benötigen dazu eine stärkere Vertrauenskultur zwischen den Sicherheitsbehörden und den Unternehmen. Gegenseitiges Vertrauen ist die zentrale Grundlage für einen konstruktiven Dialog und gemeinsames Handeln.

Natürlich wünschen wir uns in diesem Zusammenhang auch ein stärkeres Meldeaufkommen der Unternehmen über vermutete oder eingetretene Schadensfälle durch Spionage oder elektronische Angriffe. Insofern begrüße ich die laufenden Initiativen zum Erlass eines neuen IT-Sicherheitsgesetzes, welches Firmen in kritischen Wirtschaftszweigen (darunter Energienetze, Bank- und Geldsysteme sowie die Telekommunikation) zur Meldung verpflichtet, wenn sie Opfer schwerwiegender Cyberangriffe geworden sind.

Im besonderen Fokus der Security-Awareness des BfV stehen forschungsintensive und innovative Unternehmen, die ihr essenzielles Firmen-Know-how – die sog. „Kronjuwelen“ – nur unzulänglich schützen.

Aber gerade diese Unternehmen tragen wesentlich dazu bei, dass „Made in Germany“ nach wie vor Weltruf genießt und Deutschland sich Vize-Exportweltmeister nennen kann.

Sie verfügen häufig über Verantwortliche z.B. für Entsorgung oder soziale Belange, aber in der Regel nicht über Sicherheitsverantwortliche, die auch für den Informations- und Know-how-Schutz zuständig sind.

Sicherheit sollte aber ebenso ein Unternehmensziel sein, zum Schutz des Unternehmens, seiner Mitarbeiter und der schon erwähnten „Kronjuwelen“.

„Business Continuity“ ohne Sicherheit ist ein Vabanquespiel.

Hier setzen wir an und bieten unter dem Leitmotiv „Prävention durch Information“ differenzierte Sensibilisierungsangebote an. Neben zielgruppengenauen Sicherheitsvorträgen und bilateralen Sicherheitsgesprächen – unter weitreichendem Vertrauensschutz – zählen dazu handlungsorientierte Informationsschriften, ein regelmäßiger Newsletter, Messeauftritte und natürlich auch unsere jährliche Sicherheitstagung.

Eine „human Firewall“ ist eine unabdingbare Ergänzung für sichere IT- und Kommunikationstechnik in den Unternehmen.

Die Bedeutung des Faktors Mensch für ein funktionierendes und nachhaltiges Sicherheitsmanagement unterstreichen der Unternehmensberater Fred Maro sowie Manfred Jilg von der ASW in ihren Beiträgen. Ich freue mich sehr, dass wir diese beiden Experten für unsere heutige Tagung gewinnen konnten.

Um innovative mittelständische Unternehmen – das Rückgrat der deutschen Industrie – noch zielgenauer zu sensibilisieren, haben wir uns am 7. April mit dem Verband der deutschen Maschinen- und Anlagenbauer VDMA auf eine Kooperation für mehr Wirtschaftsschutz verständigt.

Hierzu ist vorgesehen, individuelle Sensibilisierungs- und Informationsangebote für Unternehmen in einem der wichtigsten und umsatzstärks-

ten Wirtschaftszweige zu entwickeln und durch gemeinsame öffentlichkeitswirksame Aktivitäten zu begleiten.

Kernzielgruppe sind die sog. „Hidden Champions“ – hochinnovative deutsche Weltmarktführer – die verstärkt im Zielspektrum von Wirtschaftsspionage und Konkurrenzausspähung stehen.

Die Zusammenarbeit des BfV mit dem VDMA ist damit ein konstruktiver Beitrag für mehr Kooperation von Staat und Industrie, für mehr Wirtschaftsschutz und ein weiterer Meilenstein auf dem Weg zu einer effektiven und zielgenauen nationalen Wirtschaftsschutzstrategie.

Ich appelliere an Sie: Nutzen Sie diese Chance zum Informationsaustausch. Nutzen Sie auch unser Angebot für Sensibilisierungsaktivitäten unter dem Leitmotiv „Prävention durch Information“.

Wir alle sollten unseren Teil dazu beitragen, die Vertrauenskultur im Sinne der gemeinsamen Erklärung von Bundesregierung und Wirtschaftsverbänden zu stärken. Wirtschaftsschutz dient allen –den Unternehmen, den Beschäftigten und auch dem Staat.

Letztlich geht es stets um den Schutz Ihrer „Kronjuwelen“. Erhöhte Cyber-Sicherheit bedeutet dagegen insgesamt mehr Freiheit. Wer sicherer kommuniziert, kommuniziert und agiert freier!

Ich danke Ihnen für Ihre Aufmerksamkeit und freue mich nun auf eine ertragreiche Veranstaltung.

Vortrag „ASW Kompetenz-Center-Modell als Unterstützung für einen Wirtschaftsschutz durch Qualifikation“

Manfred Jilg; Direktor Standortsicherheit, BASF SE, ASW-Vorstandsmitglied

Bei der Vorstellung des Verfassungsschutzberichtes 2013 führte der Bundesinnenminister aus:
„Die Spionageabwehr ist eine zentrale Aufgabe des Verfassungsschutzes. Fragen der Cybersicherheit und Cyberabwehr werden neue Arbeitsschwerpunkte des Ministeriums und auch der Sicherheitsbehörden sein. Handlungsbedarf steht jedoch nicht nur auf der Seite des Staates sondern auch auf der Seite der Unternehmen. Wirtschaftsschutz steht mehr denn je auf der sicherheitspolitischen Agenda.“ [1]

Um dieser Forderung Rechnung zu tragen, kommt es aus Sicht der Arbeitsgemeinschaft für Sicherheit der Wirtschaft (ASW) unter anderem darauf an, Unternehmen bei der Qualifizierung und Ausbildung der Verantwortungsträger für Sicherheit zu unterstützen. Für dieses Ziel setzt sie sich seit mehreren Jahren der ASW-Arbeitskreis Aus- und Weiterbildung ein. Dessen Hauptaufgaben bestehen in der Mitwirkung bei der Entwicklung neuer Sicherheitsberufe sowie in der Beratung und Unterstützung von Universitäten und Hochschule bei der Implementierung von Studiengängen im Sicherheitsmanagement. Neben dem Engagement im Bereich der Weiterbildungsverordnungen wie zum Beispiel Meister für Schutz und Sicherheit, erstellt der AK Positionspapiere zu allen sicherheitsrelevanten Fragestellungen in Zusammenhang mit der Aus- und Weiterbildung von Fach- und Führungskräften. Die Mitgliederstruktur der ASW, bestehend aus den regionalen Sicherverbänden und vielfältigen Branchenverbänden, macht es möglich, sowohl die Leitungsebenen wie auch die Fachebenen aus den deutschen Unternehmen anzusprechen. Mit den 2013 geschaffenen Kompetenz-Centern trägt die ASW zur Stärkung des Wirtschaftsschutzes bei. Die Themen reichen von Lage und Reisesicherheit über Anti-Fraud-Management bis zum Wirtschaftsschutz und Spionageabwehr, um nur ein paar der zahlreiche Themen zu nennen.

Im Bereich Aus- und Weiterbildung wollen wir Sicherheitsqualifikationen in Kooperation mit etablierten Anbietern koordinieren und durchführen. Neue Herausforderungen wie Cyberangriffe aber auch Social Engineering machen die Weiterentwicklung von zeitgemäßen Aus- und Weiterbildungsmöglichkeiten für die Sicherheitswirtschaft notwendig. Darüber muss es, auch im Sinne des verbesserten unternehmensseitigen Wirt-

1 Veröffentlicht von SecuMedia am 18.Juni 2014

schaftsschutzes, um einen Bewusstseinswandel in der Wirtschaft in Bezug auf Gefährdungspotentiale und deren Risikominimierung gehen. In Behörden wie in Unternehmen führen mangelnde Kenntnis über Aufgaben und Fähigkeiten des jeweils anderen sowie die Befürchtung von Reputationsverlusten zu einer optimierbaren Vertrauenskultur. Mit Informations- und Erfahrungsaustauschprogrammen wollen wir dem entgegentreten. Zur Unterstützung, insbesondere der mittelständischen Unternehmen, soll eine Plattform zum Austausch von Awareness-Kampagnen im Sinne von best practise aufgebaut und betrieben werden.

Jedes vierte Unternehmen ist Opfer von Wirtschaftskriminalität. Dazu kommt eine internationale Studie von Ernst& Young an der auch 50 Unternehmen aus Deutschland teilnahmen.[2] Daraus aber abzuleiten, dass die kleinen und mittelständischen Unternehmen keine Awareness für Wirtschaftskriminalität haben, wäre zu kurz gegriffen. Oftmals ist die Awareness durchaus vorhanden, es fehlen jedoch die notwendigen Ressourcen oder die Priorisierung der anstehenden Aufgaben steht einer direkten Handlung entgegen. Den fehlenden Ressourcen ist mit Unterstützungsangeboten in der Qualifizierung zum Wirtschaftsschutz entgegenzutreten. Den Teilnehmern/den Unternehmen muss ein Mehrwert geboten werden, der mit einem übersichtlichen Zeitansatz gehoben werden kann. Dabei geht es zum Beispiel darum, dass die verantwortlichen Personen die Notwendigkeit bzw. die Inhalte einer Beratungsleistung erkennen bzw. festlegen können, und nicht darum, dass sie im eigenen Unternehme selbst eine fachlich fundierte Analyse erstellen können.

Einen ersten Ansatz für Unternehmensvertreter gibt es dazu an der Fachhochschule Campus Wien in Österreich. Hier entwickelten Mitarbeiter der FH unter Leitung von Professor Langer in Kooperation mit dem österreichischen Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) einen Ausbildungsgang „Wirtschaftsschutz mit System“. Sowohl das deutsche Bundesamt für Verfassungsschutz wie auch Vertreter der ASW haben in Kooperation bei der Durchführung des ersten Seminardurchgangs mitgewirkt. Der Fokus der deutschen Teilnehmer lag auch darauf, zu überprüfen, in wieweit die Ausbildungsinhalte und Rahmenbedingungen für die Implementierung im bundesdeutschen Umfeld geeignet erscheinen.

BfV und ASW arbeiten derzeit gemeinschaftlich an der Entwicklung eines bedarfsgerechten Lehrgangs „ Manager/-in Wirtschaftsschutz“. Als Zielgruppe sind hier besonders die kleinen und mittleren Unternehmen in Deutschland (KMU) sowie die Nachwuchsführungskräfte zu erwähnen. Die Durchführung soll mit renommierten Weiterbildungsträgern, Universitäten und Fachhochschulen weitgefächert ausgerollt werden. Absicht ist es, noch 2014 ein Pilotseminar an den Start zu bringen. Zunächst sollen innerhalb des einwöchigen Lehrgangs, eine Splittung in 2 Teilabschnitte ist

2 Quelle: Ernst und Young. Veröffentlicht SecuMedia 17.06.2014

möglich, inhaltlich die Bedeutung von Wirtschaftsschutz und die Differenzierung von Wirtschafts- und Industriespionage herausgearbeitet werden. Den Teilnehmern sollen relevante Rechtsvorschriften ebenso wie die grundlegenden Angriffsmuster und Akteure im Phänomenfeld Wirtschafts- und Industriespionage dargestellt werden. Dazu gilt es für das eigene Unternehmen hilfreiche Präventionsmaßnahme zu erkennen, in dem die Anforderungen an den physischen Grundschutz, die Grundlagen des Geheim und Sabotageschutzes sowie die Rahmenbedingungen für Personenüberprüfung von Experten vermittelt werden. Weiterhin werden die Fähigkeiten zur Durchführung einer Bedrohungsanalyse sowie des Erkennens genereller Gefährdungen für das eigenen Unternehmens durch Mitarbeiter, Kunden und Kontraktoren z.B. durch Social Engineering trainiert. Grundlegend werden dabei auch die Aufgaben, Zuständigkeiten und Unterstützungsmöglichkeiten der Sicherheitsbehörden und der Verbände aufgezeigt. Die Aufgaben der zukünftigen Manger/-innen Wirtschaftsschutz im eigenen Unternehmen sollen sich später wie folgt darstellen:

+ Awareness für Wirtschaftsschutz im Management schaffen (Relevanz),
+ Sinn und Notwendigkeit für Maßnahmen vermitteln (Akzeptanz)
+ Ziele für den Schutz vor Wirtschafts- und Industriespionage für das eigene Unternehmen identifizieren, analysieren, bewerten, (Früherkennung)
+ angemessene Maßnahmen ableiten und Restrisiko transparent machen (Schutz)

Im Rahmen der Zusammenarbeit in der Steuerungsgruppe Wirtschaftsschutz und deren Expertengruppen zur Erarbeitung einer nationalen Wirtschaftsschutzstrategie wird die Einbettung des Lehrgangs geprüft.

Zentralorganisation der Wirtschaft

BfV/ASW-Sicherheitstagung zum Thema

"Proaktiver Wirtschaftsschutz: Prävention durch Information"

ASW Kompetenz-Center-Modell

Wirtschaftsschutz durch Qualifikation

Manfred Jilg
ASW Vorstandsmitglied

03.07.2014/Stand:0

ASW Kompetenz- Center Modell

Deloitte. Partner der

POWER Förderer der

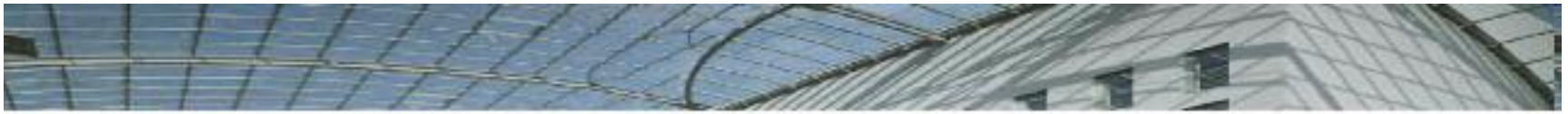
Agenda

1. Zusammensetzung und Aufgaben des ASW Kompetenzzentrums Aus- und Weiterbildung

2. zukünftige Herausforderungen und Einbindung in das Kompetenz-Center-Modell der ASW

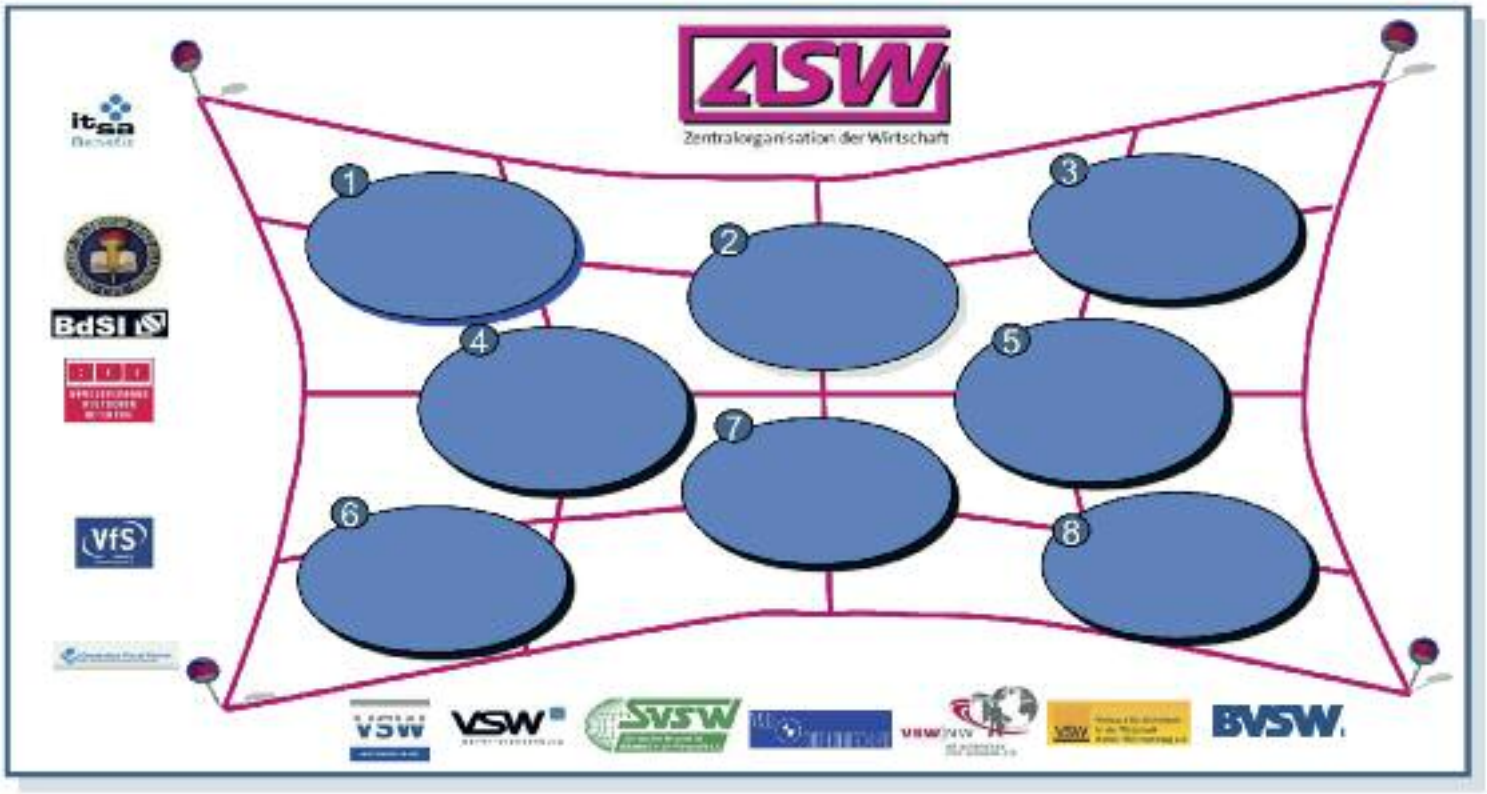
3. Kurzbericht zur Mitwirkung im Pilotprojekt Wirtschaftsschutz mit BVT, BfV und FH Campus Wien

4. Qualifikation Manager/-in Wirtschaftsschutz für KMU in Deutschland



3

Das Kompetenzzentrum Aus- und Weiterbildung setzt sich aus den Vertretern der Mitgliedsverbände zusammen



Kompetenzzentrum Aus- & Weiterbildung

Aufgabenspektrum:

- Mitwirkung als betriebliche Experten und Sozialpartner bei der Entwicklung der neuen Ausbildungsberufe
- wesentliche Mitarbeit bei der Weiterbildungsverordnung zur IHK geprüften Schutz- & Sicherheitskraft, Meister für Schutz und Sicherheit
- Zusammenarbeit mit Universitäten und Hochschulen bei der Implementierung von Studiengängen Sicherheitsmanagement
- Kooperation mit Weiterbildungsträgern
- Initiierung von Veränderungen in der gewerberechtlichen Zulassungsvoraussetzungen
- Erstellen von Positionspapieren zu allen Fragen der Aus- & Weiterbildung

ASW
Zentralorganisation der Wirtschaft

Das Projekt KCM begleitet die Umsetzung des Kompetenz-Center-Modells.

Kompetenzzentrum Sicherheitstrainings & Awarenessakademie

7

Zielsetzung Sicherheitstrainings:

– Koordination und Durchführung von Sicherheitsqualifikationen in Kooperation mit etablierten Anbietern aus dem Trainingsbereich.

– Weiterentwicklung von Zertifikaten und Schaffung neuer zeitgemäßer Ausbildungs-/Qualifikationsformen für die Sicherheitswirtschaft

Kernaspekte für die Umsetzung:

- Erfassung / Bewertung aller Angebote (Inland + Europa)
  => Dopplungen vermeiden
- Ableitung ASW-Lastenheft
- Ansprechpartner politische Verordnungen / Gesetze
- ASW-Bildungsangebot CreditPoints (Prüfung, Realisierung)
- Koordinator Behörde / Wirtschaft (z.B. BfV)
- E-Learning

ASW Kompetenzzentrum Sicherheitstrainings & Awareness Akademie

Zielsetzung Awareness Akademie:

– Schaffung eines Bewusstseinswandels in der Wirtschaft hinsichtlich der Gefährdungslage und der Möglichkeiten zur Minimierung der damit einhergehenden Risiken.

– Förderung einer stärkeren Vertrauenskultur, um die Kooperation von Sicherheitsbehörden und Wirtschaft zu intensivieren, den Informations- und Erfahrungsaustausch zu stärken und Reputationsängste bei den Unternehmen abzubauen.

– Aufbau und Betrieb einer Plattform für Awareness Kampagnen. Unternehmensübergreifender Austausch von Kampagnen (best practise)

Wesentliche Erfolgskriterien:

- Content-Plattform
  - Behörden
  - Mitglieder
- Katalogisierung
- Empfehlung

Presse Wirtschaftsschutz

9

Jedes vierte deutsche Unternehmen Opfer von Wirtschaftskriminalität

Zu diesen Ergebnissen kommt eine Studie der Prüfungs- und Beratungsgesellschaft EY (Ernst & Young), für die mehr als 2700 Vorstandsvorsitzende, Finanzvorstände, Leiter der Revision, der Rechtsabteilung und des Compliance Managements aus 59 Ländern befragt wurden, davon 50 aus Deutschland.

Quelle: Ernst & Young
Veröffentlicht von SecuMedia am 17. Juni 2014.

..."Das wichtigste Kapital der Unternehmen ist ihre Innovationsfähigkeit, daher fürchtet der Mittelstand am meisten um seine Wissensträger. Rund drei Viertel der Befragten hält Mitarbeiter und Management für besonders gefährdet, Opfer krimineller Angriffe zu werden..."

Auszug aus der Presseermittelung des Sicherheitsmelders

ASW
Zentralverband der Wirtschaft

Manager/In Wirtschaftsschutz

11

Ausbildung „ Wirtschaftsschutz mit System“

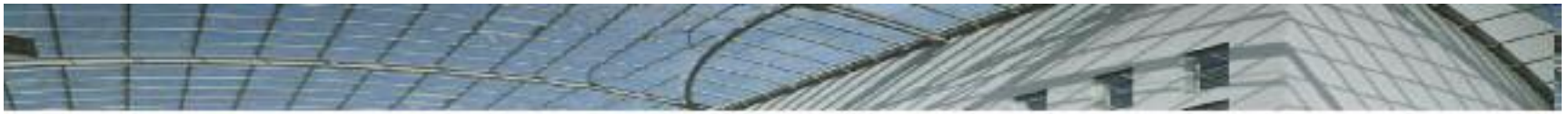
In Kooperation mit dem BfV und BVT

Durchführung eines Seminars Version 1 in Zusammenarbeit des BVT und der FH Campus Wien 1. Quartal 2014

Qualifikation Manager/-in Wirtschaftsschutz für KMU in Deutschland

13

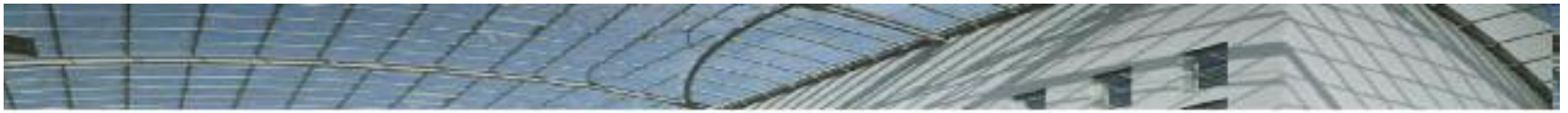
- Mitwirkung in der Steuerungsgruppe Wirtschaftsschutz
- Entwicklung eines bedarfsgerechten Lehrgangs Manager/In Wirtschaftsschutz,
- Zielgruppe:
  - KMU in Deutschland,
  - Nachwuchsführungskräfte
- Zusammenarbeit mit renommierten Weiterbildungsträgern, Universitäten , Fachhochschulen



Qualifikation Manager/-in Wirtschaftsschutz für KMU in Deutschland

Möglicher Rahmenplan

- Bedeutung von Wirtschaftsschutz und Differenzierung von Wirtschafts- und Industriespionage
- Grundlegende Angriffsmuster (modus operandi) und Akteure in der Wirtschafts- und Industriespionage.
- Überblick über relevante Rechtsvorschriften
- Hilfreiche Präventionsmaßnahmen für die eigene Organisation (best practise)
- Anforderungen an physischen Grundschutz, Grundlagen des Geheimschutzes und Rahmenbedingungen für Personenüberprüfungen



15

Qualifikation Manager/-in Wirtschaftsschutz für KMU in Deutschland

Inhalte:

– Durchführung einer Bedrohungsanalyse

– Aufgaben ,Zuständigkeiten und Unterstützungsmöglichkeiten von Sicherheitsbehörden und Verbänden.

– Schnittstellen zu CyberSecurity, Produktpiraterie, Informationsschutz,..

– Gefährdung des eigenen Unternehmens durch Mitarbeiter, Kunden, Kontraktoren (Social Engineering)

– Erstellung eines Pflichtenheftes für Beratungsaufträge

Qualifikation Manager/-in Wirtschaftsschutz für KMU in Deutschland

Kompetenzen der Lehrgangsteilnehmer zur Beratung des Managements

–Awareness für Wirtschaftsschutz im Management schaffen (Relevanz)

–Sinn und die Notwendigkeit für die Maßnahmen vermitteln (Akzeptanz)

–Ziele für den Schutz vor Wirtschafts- und Industriespionage im Unternehmen implementieren (Strukur)

–Gefahren aus Wirtschafts- und Industriespionage für die das Unternehmen identifizieren, analysieren, bewerten (Früherkennung)

–Angemessene Maßnahmen ableiten und Restrisiko transparent machen (Schutz)

Qualifikation Manager/In Wirtschaftsschutz für KMU in Deutschland

Kompetenzen der Lehrgangsteilnehmer zur Beratung des Managements

- Implementierung eines Berichtswesens mit Eskalationswegen
- Nachbereiten relevanter Vorfälle (PDCA-Zyklus)
- Aufbau einer QM-Systems (Audit, Nachhaltigkeit)
- Erkennen und Abstellen von Schulungs-/Awarenessdefiziten

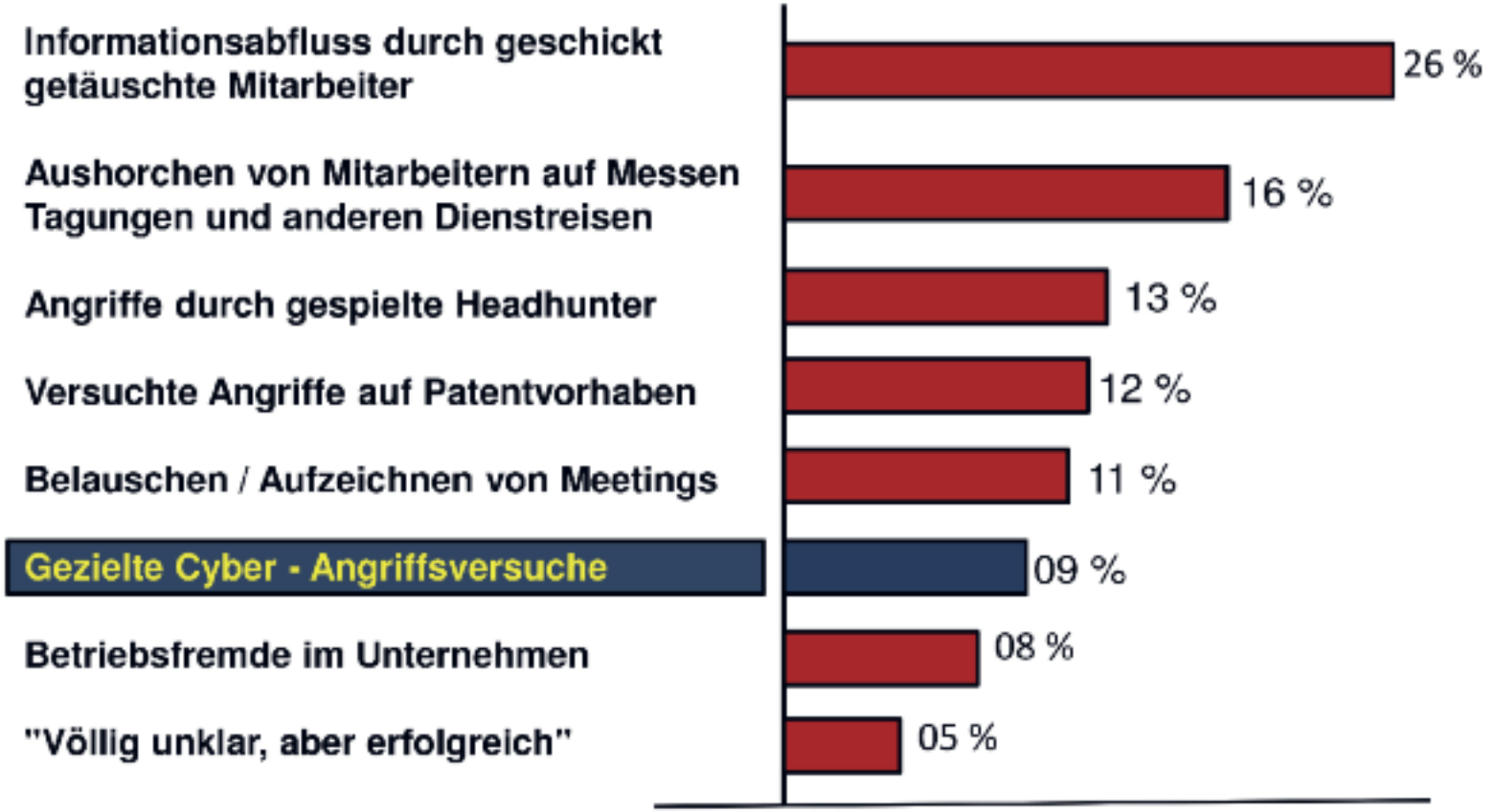
ASW
Zentralverband der Wirtschaft

Industriespionage – unterschätzte Gefahr!
Handout zum
gleichnamigen Vortrag
von und mit
Fred Maro
Geschäftsführer
www.fm-nospy.com

Nicht repräsentativ – trotzdem aufschlussreich!

FM-nøspy

"Was ist konkret passiert?"



Ref: FM-nospy 2013 /
122 befragte angegriffene Unternehmen

"Planen Sie jetzt konkrete Schutzmaßnahmen?"

FM-nøspy

"Nein, denn wir wissen ziemlich genau, wer das war."

"Unsere Mitarbeiter passen schon auf!"

"Bei uns haben alle Compliance Regeln unterschrieben."

"Unsere IT ist ja sicher!"

"Wir haben im Moment andere Prioritäten."

"Wozu – die Sachen sind ja schon weg!"

Ref: FM-nospy 2013 /
122 befragte angegriffene Unternehmen

Verblüffende Feststellung

FM-nøspy

Alle reden von "Cyberwar" und IT-Angriffen …

Unsere Erfahrung ist:

Der weitaus größte Teil der Angriffe erfolgt durch "klassisches Social Engineering"!

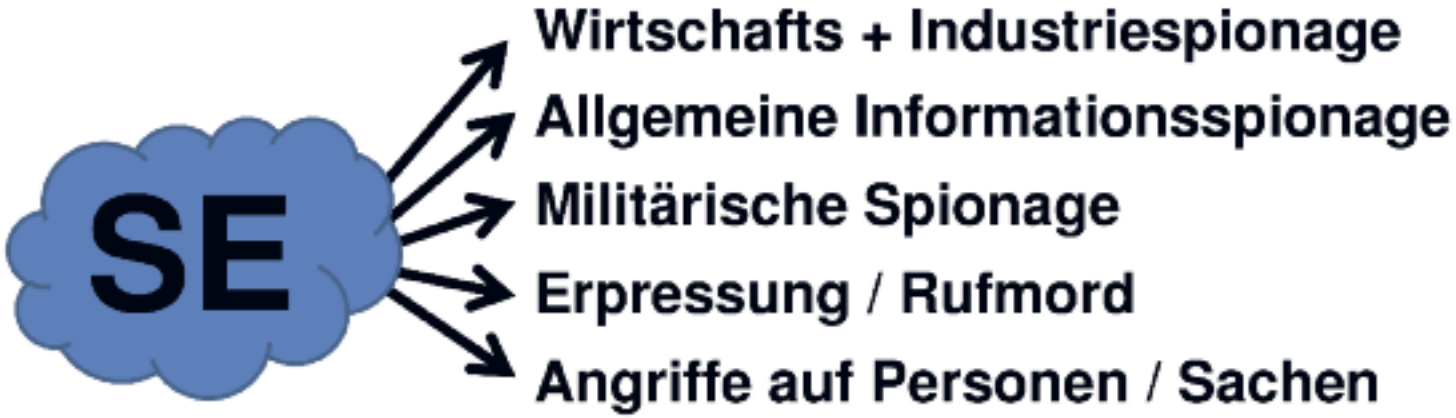
Unsere Erkenntnis ist:

Die meisten kennen den Begriff, jedoch wissen nur sehr wenige, wie das eigentlich wirklich funktioniert!

Industriespionage → “Social Engineering“

“Social“ = “Soziales“ / “Engineering“ = “etwas zusammenbauen“

Das (Aus-)nützen natur-gegebener menschlicher Stärken und Schwächen, um (Teil-) Informationen für weitergehende Spionage-Aktivitäten zu erhalten.



3 grundsätzlich unterschiedliche Techniken

“Social Engineering“ ist KEIN reines IT-Thema!!!

“DATA-BASED“ Social Engineering

z.B. Erschleichen von Passwörtern, Stehlen von Token,
→ gezielte Suche nach Dokumenten

“REVERSED“ Social Engineering

Verursachen von Schaden
→ Angriff in der Rolle von Helfern !

“HUMAN-BASED“ Social Engineering

Informationsspionage durch direkte Kommunikation

"Human based Social Engineering"

… erlebt Anerkennung als hoch kompetent und “gefragt“
… erlebt "die teure Welt der Topmanager"
… liefert gerne Hintergrundwissen, um gegenüber dem Headhunter kooperationsbereit zu erscheinen und ihm seine Arbeit zu erleichtern …

Mitarbeiter(in)

“Headhunter“

ACHTUNG!
So gut wie nie überprüfen Angesprochene die Identität des “Headhunters“

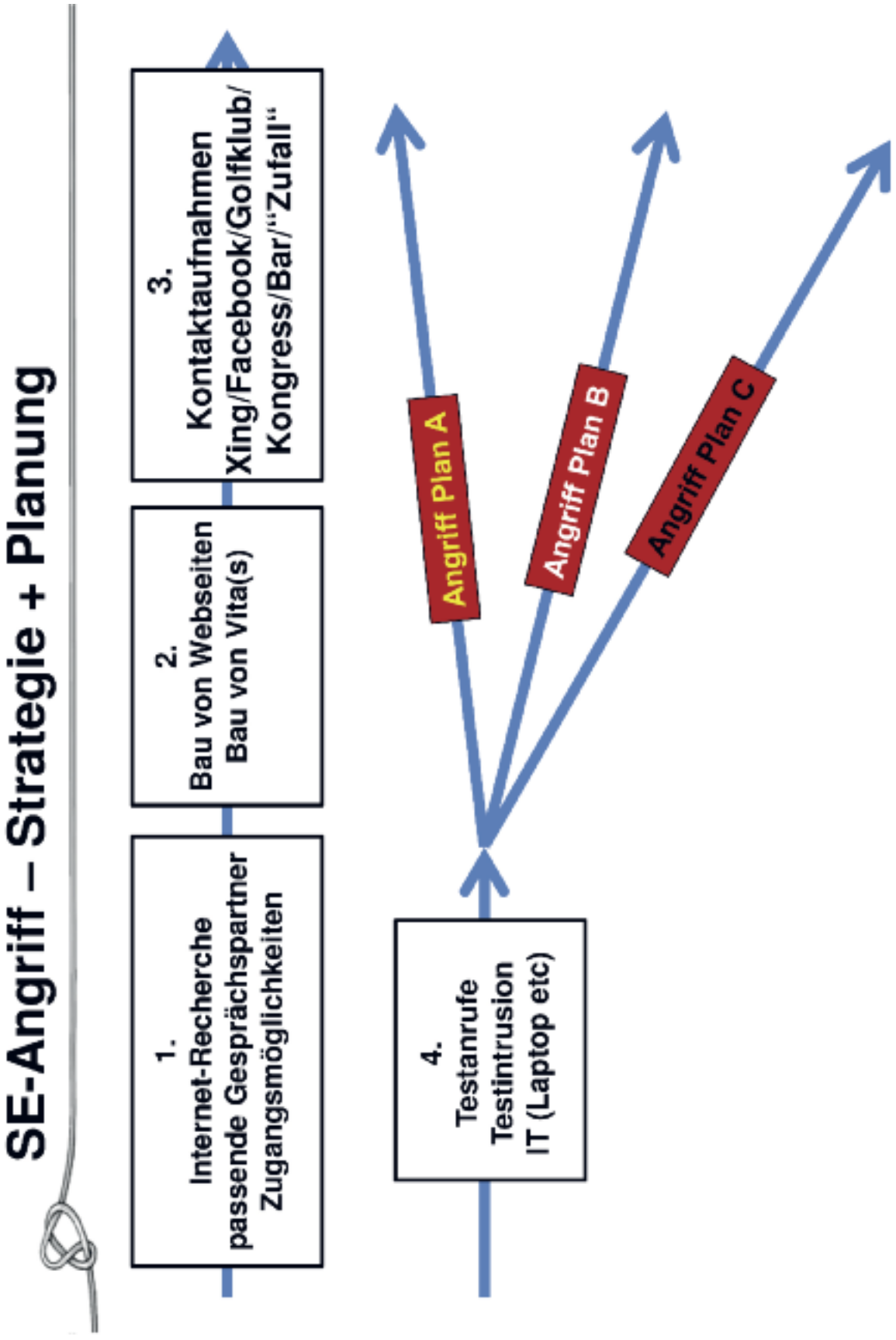
Wie wird ein “klassischer“ Angriff üblicherweise strategisch geplant?

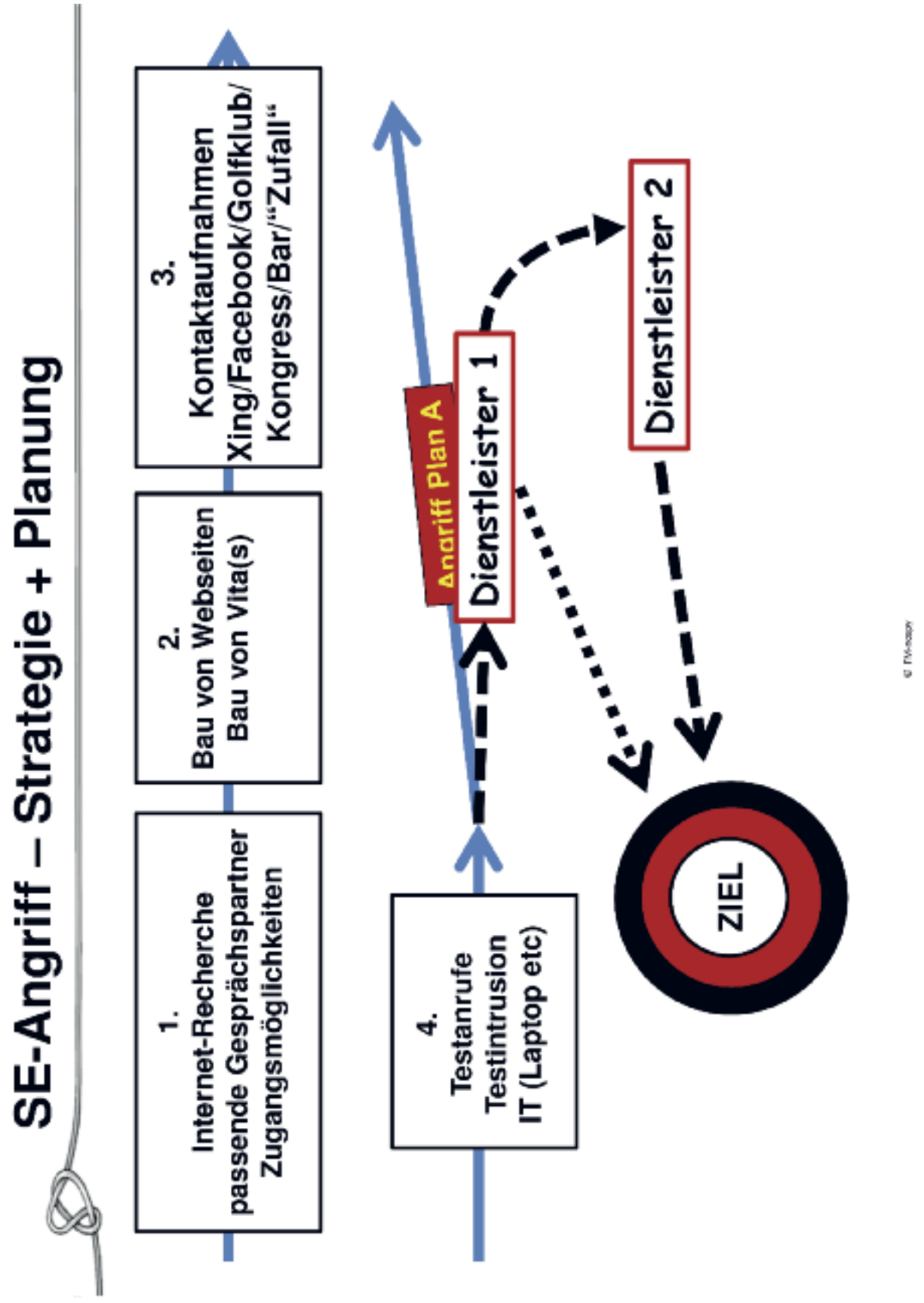
Interessent erteilt Auftrag …

SE – Wer sind klassische Angreifer?

1. **Konkurrenten oder Mitanbieter**
   (via beauftragte, oft obskure “Detekteien“ od. “Business Intelligence“)
2. **Journalisten** ("Bad News = Good News")
3. **Diffuse Angreifer** (Spekulanten / Fahnder / Stalker)
4. **Frustrierte Mitarbeiter** (Leichtsinn/Revanche/"Eintrittsgeschenke")
5. **Freie Informationshändler**
6. **Kriminelle Banden** (Erpressung / Raub / Diebstahl)

Weniger als 5% der beauftragten Angreifer werden ertappt!


SE-Angriff – Strategie + Planung
1.
Internet-Recherche
passende Gesprächspartner
Zugangsmöglichkeiten
2.
Bau von Webseiten
Bau von Vita(s)
3.
Kontaktaufnahmen
Xing/Facebook/Golfklub/
Kongress/Bar/"Zufall"
4.
Testanrufe
Testintrusion
IT (Laptop etc)
Angriff Plan A
Angriff Plan B
Angriff Plan C


SE-Angriff – Strategie + Planung
1.
Internet-Recherche
passende Gesprächspartner
Zugangsmöglichkeiten
2.
Bau von Webseiten
Bau von Vita(s)
3.
Kontaktaufnahmen
Xing/Facebook/Golfklub/
Kongress/Bar/“Zufall“
4.
Testanrufe
Testintrusion
IT (Laptop etc)
Angriff Plan A
Dienstleister 1
Dienstleister 2
ZIEL


Warum funktioniert
Social Engineering so gut?

Wir kennen das Vertrauliche nicht!

Vertraulich ist alles,
was nicht einfach im Internet zu finden ist!

Urlaubszeiten / Urlaubsorte / Abteilungsnamen / Projektmanager
Telefonnummern / Roadmaps / Kongressteilnahmen / Reisepläne
Zahlungsprozedere / Spitznamen / Service Level Agreements
Vorstandsprotokolle / Hobbys / Lagerorte / Dienstleister-Namen
Tagungsorte / Tagung-Agenda / Formulare / Strategien / Hauspost
Abfallmanagement / Zugangswege / Zwischenfälle / Ausweise
Urlaubsvertretungen / Autokennzeichen / Passwörter
Namen von Schlüsselpersonen / Namen von Beratern
und vieles ähnliches mehr …

Wir haben keine Zeit, aufmerksam zu sein !

Viele Mitarbeiter sind völlig "übertaktet" !
Sie reagieren nur noch, anstatt zu "agieren"!

Die Systeme, die Aufmerksamkeit verlangen, gestatten keine Zeit für Hinschauen und Nachfragen …

Wir beurteilen nach Klischees!

… eine Folge von Zeitmangel + Reizüberflutung

Wie sieht ein "Manager aus" ?

Wie sieht eine "Venus- oder Adonisfalle" aus ?

Wie sieht ein "IT-Fachmann" aus?

Wie sieht ein "Araber / Asiate / Afrikaner" aus?

Wie spricht ein "Ausländer" ?

Wer pflegt welchen Akzent ?
etc.

Wir sind – untrainiert – Profis nicht gewachsen!

Wir geben viel Geld für Verkaufstraining aus!

Wir geben kein Geld aus, um die Wächter unserer Kronjuwelen fit zu machen, in Telefonaten gegen Psychologen zu bestehen.

Wir geben kein Geld aus, um Dienstleister und Zulieferer zu überprüfen und zu schulen.

… wir machen teures E-Learning, damit wir Zeit sparen …

Nachdenkenswertes

FM-nøspy

- **Unterschätzen wir vielleicht die Angriffshäufigkeit, weil wir Angriffe oft gar nicht bemerken?**
- **Konzentrieren wir uns leichtsinnigerweise fast nur auf die IT-Seite der Industriespionage?**
- **Ignorieren wir, dass der größte Teil der SE-Angriffe über – nichts Böses ahnende – Dienstleister oder Zulieferer läuft?**
- **Investieren wir mehr in, oft ineffiziente Tagungen als in den wichtigen Schutz unserer Kronjuwelen?**

Nachdenkenswertes …

FM-nøspy

- **Glauben wir, dass Compliance-Regeln und Mails zum Thema Geheimschutz reichen?**
- **Vergessen wir nicht oft, dass Aufmerksamkeit sehr viel mit Unternehmenskultur und "Spaß haben" zu tun hat!**
- **Beschäftigen wir uns vielleicht zu viel mit Statistiken, anstatt unsere Mitarbeiter zu dem zu machen, was Spionen das Leben wirklich schwer macht:**

Eine engagierte "menschliche Firewall" !

versuchen Sie folgenden kleinen Test!

Stellen Sie in einer Unterhaltung eine bewusst leicht falsche Behauptung auf!

Sie können sicher sein, dass Sie umgehend korrigiert und berichtigt werden …

… und damit Tatsachen erfahren …


FM-nospy
Vielen Dank für Ihre
aufmerksame Teilnahme!

Bundesamt für Verfassungsschutz

BfV Bundesamt für Verfassungsschutz



Elektronische Angriffe auf die Wirtschaft

Die Gurtpflicht

- 1976 eingeführt
- Damals Widerstände
- Heute eine Selbstverständlichkeit

Bundesamt für Verfassungsschutz

IT-Sicherheit

- IT-Sicherheit wird als störend empfunden
- IT-Sicherheit bindet Personal und kostet Geld
- Teilweise ist die Infrastruktur nicht mal bekannt
- Outsourcing der Dienstleistung
- Sicherheitskonzepte / Regelungen für Passwörter
- Zuständige Person im Urlaub

Sicherheitsbewusstsein

- Sehr unterschiedlich ausgeprägt
- Unternehmen sind oft überrascht, wenn Vorfall bekannt wird
- Sicherheitsbewusstsein muss bei der Führungsebene ankommen
- Umgang mit Daten
  - Wichtig für Angriffsvorbereitung!

Bundesamt für Verfassungsschutz

Umgang mit Daten

- Jobbörsen
  - Können Aufschluss über eingesetzte Technik geben
- Soziale Netzwerke
  - Preisgabe von Firmenwissen
  - Fake-Profile
- Teilweise Verlust über Datenhoheit

Bundesamt für Verfassungsschutz

Folgen eines Angriffs

- Angreifer möchte Vollzugriff auf System
- Informationsgewinnung → Spionage
- Bereinigung oft sehr schwierig und kostenintensiv
- Übergang zu Sabotage durch wenige Mausklicks!

Bundesamt für Verfassungsschutz

Kritische Infrastrukturen

- Derzeit abstrakte Gefahr
- Steigerung der Gefahr durch grundlegende Veränderungen insbesondere außenpolitischer Entwicklungen

Aktuelle Lage

- Angreifer hat es oft sehr leicht
- Das eingesetzte Schadprogramm wird in der Regel nicht detektiert
- Informationen über Angriffe bleiben oft nur bei dem angegriffenen Unternehmen
- Das hat zur Folge, dass der Angreifer über Jahre dieselbe Infrastruktur für Angriffe nutzen kann

Angriffsmethoden

- Emails mit verseuchten Anhängen
- Verseuchte Homepages
- Infizierte Mobile Datenträger:
  - » USB-Sticks
  - » externe Festplatten
  - » Speicherkarten
  - » MP3-Player
  - » Laptops
  - » Smartphones

Angriffsmethoden

Bsp.: „Watering Hole“

- Der Angreifer untersucht das Verhalten des Opfers (Facebook, Twitter ….)
- Er findet heraus, dass die Mitarbeiter oft beim örtlich ansässigen Italiener online bestellen
- Angreifer manipuliert Homepage des Restaurants und wartet.
- Opfer ruft Seite des Restaurants auf und infiziert sich
- Angreifer filtert (IP-Adressen, Spracheinstellungen etc.)

Branchen

- Forschungszentren
- Automobilbranche
- Satellitenunternehmen
- Rüstungsbranche
- Zulieferbetriebe
- Luftfahrt
- ....

Bundesamt für Verfassungsschutz

Angreifer

- Nachweis ist schwierig
- Verschleierungen
- Alle nutzen die gleiche Technik
- 360 Grad-Blick daher von wesentlicher Bedeutung

Was macht der Verfassungsschutz?

Zuständigkeit

- EA mit nachrichtendienstlichem Hintergrund

- EA durch extremistische/terroristische Bestrebungen

Bundesamt für Verfassungsschutz

Was macht der Verfassungsschutz?

- Ausbau der Kapazitäten
- Neue Arbeitseinheit für die Bearbeitung von Angriffen auf die deutsche Wirtschaft
- Nationale und internationale Kooperationen
- Allgemeine Sensibilisierungen

Bundesamt für Verfassungsschutz

Was macht der Verfassungsschutz?

Unterstützung im konkreten Fall:

- ND-Bewertung
- Ermittlung Verursacher
- Bereitstellen von Hintergrundinformationen
- Wesentliches Ziel: Feststellung von betroffenen deutschen Unternehmen

Bundesamt für Verfassungsschutz

Was macht der Verfassungsschutz?

- **Ziel:**
  - Tatsächlicher Schutz für die Wirtschaft
  - Angriffe sollen durch Unternehmen erkannt werden können
  - Zeitnahe Erstunterrichtung
  - Erweiterung der Datenbasis

- **Problem:**
  - Angriffe werden Sicherheitsbehörden selten mitgeteilt

Bundesamt für Verfassungsschutz

Fazit

- Angriffe gegen deutsche Unternehmen sind Realität
- Schaden für deutsche Wirtschaft
- Die Angriffe werden immer raffinierter
- Die Detektion wird immer schwerer
- IT-Sicherheit muss eine Selbstverständlichkeit werden

Angebote an die Wirtschaft

- Allgemeine Sensibilisierungen
- Unterstützung im konkreten Fall
- Zusicherung von Vertraulichkeit
- Dienstleistung ohne Gewinnerzielungsabsicht

Bundesamt für Verfassungsschutz

Vielen Dank

für Ihre

Aufmerksamkeit

Bildmaterial


ASW

Wirtschaftsschutz
ist
Teamwork