



Corporate Security

Spezialisten zum Schutz
Ihrer Mitarbeiter und
Firmenwerte

ALLIANZ FÜR
SICHERHEIT IN DER
WIRTSCHAFT

Seite **04** Interview mit
Ulrich Brehmer

PRE-EMPLOYMENT-
SCREENING

Seite **06** Interview mit
Nils Retkowski

30 JAHRE IM DIENST
DER SICHERHEIT

Seite **09** Interview mit
Wolfgang Benz



THOMAS WILDE

EDITORIAL

Corporate Security – Ein Competence Center stellt sich vor

Wenn man den Zahlen des Bundesministeriums des Inneren glauben darf, dann ist Wirtschaftskriminalität in Deutschland regelmäßig für etwa die Hälfte aller durch Straftaten entstehenden Schäden verantwortlich, obwohl sie nur etwa ein bis zwei Prozent aller Straftaten ausmacht. Obwohl es keine gesicherten Statistiken gibt und von einer hohen Dunkelziffer auszugehen ist, so kann man doch von einer Größenordnung zwischen vier und fünf Milliarden € pro Jahr ausgehen. Allein diese Zahl macht deutlich, dass es für Unternehmen von enormer Bedeutung ist, ihre Mitarbeiter und ihre Firmenwerte zu schützen. Daher haben die Bereiche Corporate Security und Compliance in den letzten Jahren immer mehr an Gewicht gewonnen.

Für Unternehmen ist es wichtig, sich hier intern richtig aufzustellen und mit geeigneten Mitarbeitern Prozesse und Strukturen zu implementieren, die sich ausschließlich diesem Zweck widmen. Und dies natürlich lautlos und ohne das laufende Geschäft zu stören.

Vor dieser sehr herausfordernden Aufgabenstellung stehen Mitarbeiter aus den Bereichen Corporate Security, Compliance und Gouvernance regelmäßig. Neben exzellentem Fachwissen brauchen sie Gespür für die Situation, Stressresistenz, Verhandlungsgeschick, Durchsetzungsvermögen und das Selbstverständnis, sich am Machbaren zu orientieren. Kenntnisse und Eigenschaften die man gezielt suchen muss.

Daher haben wir uns als renommierte Personalberatung dazu entschlossen, für dieses Umfeld und für diese speziellen Kandidatenprofile ein eigenes Competence Center ins Leben zu rufen. Mit Thomas Wilde und Thomas Hölzchen haben zwei sehr erfahrene Berater die Leitung übernommen, die als ehemalige Offiziere der Bundeswehr schon lange mit dieser Thematik vertraut sind und die in zahlreichen Projekten ein entsprechendes Netzwerk aufbauen konnten. Darüber hinaus ist es uns gelungen, einen hochkarätig besetzten Fachbeirat zu gewinnen, der uns mit seiner Expertise bereits bei der Konzeption dieses Competence Centers hilfreich zur Seite stand und der uns auch in der Projektabwicklung unterstützen kann. Ein erstes Ergebnis war die Anpassung des Suchprozesses an dieses spezielle Suchprofil. Kandidaten werden im Regelfall von zwei Beratern interviewt, grundsätzlich erfolgt ein Pre-Employment-Screening und eine Probezeitbegleitung unterstützt in der Anfangsphase der Beschäftigung.

Wir hoffen, dass wir mit der vorliegenden Broschüre ein paar Anstöße für weiterführende Überlegungen liefern können. Denn eines kann man aus den nachfolgenden Interviews immer wieder herauslesen: der Bereich Unternehmenssicherheit hat in vielen Firmen noch nicht den Stellenwert, den er eigentlich haben müsste. Und auch hieran wollen wir gerne gemeinsam mit ihnen arbeiten.

DAS COMPETENCE CENTER CORPORATE SECURITY

IHRE BERATER



Ihr Consultant Thomas Wilde

- Jahrgang 1964
- Diplom-Volkswirt
- Karriere als Offizier der Bundeswehr (u.a. zuständig für militärische Sicherheit) und in internationalen Beratungsgesellschaften
- Seit 2011 bei TOPOS
- Standort Hamburg
- Managing Partner



Ihr Consultant Thomas Hölzchen

- Jahrgang 1956
- Diplom-Kaufmann
- Karriere als Offizier in der Bundeswehr und NATO (höchste Sicherheitsstufe)
- Seit über 25 Jahren in der Personalberatung
- Seit 2015 bei TOPOS
- Standort Hamburg
- Senior Partner

FACHBEIRAT



Wolfgang Benz · Fachlicher Leiter Masterstudiengang Kriminalistik an der SHB

- Jahrgang 1965
- Diplom Verwaltungswirt, Erster Kriminalhauptkommissar aD
- Langjährige (Führungs-)Funktionen in der Hamburger Kriminalpolizei mit Schwerpunkten in der Ermittlungstätigkeit und den Spezialeinheiten
- Mehrjährige Erfahrung als Leiter der Unternehmenssicherheit eines in seinem Segment führenden Unternehmen in Hamburg
- Fachlicher Leiter und Referent im staatlich anerkannten und akkreditierten Masterstudiengang Kriminalistik an der Steinbeis Hochschule in Berlin



Nils Retkowski · COO Result Group GmbH

- Jahrgang 1978
- MBA, Offizierlaufbahn bei der Bundeswehr
- Verschiedene Führungspositionen in der Sicherheitsbranche
- COO der Result Group GmbH



Matthias Weigmann · Vorstand ANMATHO AG

- Jahrgang 1968
- Vorstand der ANMATHO AG
- IT-Security-Auditor, Datenschutzauditor, EDV-Sachverständiger


INTERVIEW MIT ULRICH BREHMER:

„ES IST IMMER WIEDER NOTWENDIG, SINN UND ZWECK UND ZIEL VON UNTERNEHMENS-SICHERHEIT DEUTLICH ZU MACHEN UND DIE KOSTEN DEM MEHRWERT GEGENÜBER ZU STELLEN.“

Was ist die Allianz für Sicherheit in der Wirtschaft (ASW)?

Die ASW ist das regionale und überregionale Netzwerk der Sicherheitsexperten aus der Wirtschaft in Deutschland. In Hamburg hat sich der Verband für Sicherheit in der Wirtschaft Norddeutschland (VSWN) bereits Ende der sechziger Jahre gegründet, im Mai dieses Jahres hat er sich in ASW Nord umbenannt. Damals wie heute dient er als Netzwerk zum Informations- und Erfahrungsaustausch der Sicherheitsverantwortlichen aus der Wirtschaft. Ein Schwerpunkt der Arbeit war immer schon das Thema „Qualifizierung“. Der ASWN bietet daher ein umfangreiches Aus- und Weiterbildungsprogramm für seine Mitglieder an. Außerdem soll in Zusammenarbeit mit der Politik und den Sicherheitsbehörden ein gemeinsames Verständnis für Sicherheit in der Wirtschaft gestärkt werden. Der ASW Bundesverband als „Verband der Verbände“ vertritt die Interessen der regionalen Allianzen für Sicherheit in der Wirtschaft gegenüber den Bundesministerien und Sicherheitsbehörden des Bundes.

Wie würden Sie das Verständnis in der Wirtschaft für Sicherheitsthemen heute einschätzen?

Man sollte annehmen, dass aufgrund der vielen Vorkommnisse und der generellen Bedrohungslage eine hohe Bereitschaft in den Unternehmen besteht, sich

mit dieser Thematik auseinander zu setzen. Nach unserer Auffassung – und da darf ich auch für den gesamten Verband sprechen – ist es aber noch nicht in ausreichendem Maße der Fall. In vielen großen Konzernen gibt es schon das Bewusstsein, für Unternehmenssicherheit zu sorgen und entsprechende Ressourcen im eigenen Unternehmen vorzuhalten beziehungsweise aufzubauen. Bei der großen Anzahl von mittelständischen Unternehmen ist dies aber noch nicht der Fall. Wir treffen immer noch auf Firmen, gerade aus dem Mittelstand, die sich gar nicht bewusst sind, dass sie eigentlich ein attraktives Ziel für Wirtschaftsspionage sind.

Wie kann ein Umdenken initiiert werden?

Es ist immer wieder notwendig, Sinn und Zweck und Ziel von Unternehmenssicherheit deutlich zu machen und die Kosten, die damit einhergehen, dem Mehrwert gegenüber zu stellen und, wo immer möglich, auch zu beziffern. Ein wenig ist es wie bei einer Versicherung. Sie zahlen eine Prämie und wenn nichts passiert ärgern sie sich, dass sie das Geld ausgegeben haben. Und dennoch wünschen Sie sich nicht, dass der Schadensfall eintritt. Bei der Unternehmenssicherheit verhält es sich ähnlich. Sie investieren in Personal, in Technik und in Know-how und versuchen so, die Risiken zu minimieren. Tritt kein Schaden ein,

stellt sich die Unternehmensleitung schon die Frage, ob sie nicht gegebenenfalls zu viel Geld in die Hand genommen hat. Hier ist es wichtig, dass die Sicherheitsverantwortlichen in den Unternehmen immer wieder auch auf die Risiken hinweisen und welche Abwehrmöglichkeiten es gibt, um schlussendlich auch den Mehrwert darzustellen, den das Unternehmen aus dem Schutz und der Sicherheit seiner Firmenwerte zieht.

Wo sehen Sie die Bedrohungslage für einen mittelständischen Unternehmer?

Diese Frage ist nicht generell zu beantworten, denn es kommt natürlich auf die Branche an, in der sie tätig sind. Wenn man sich die großen Trends der Vergangenheit ansieht, dann kann man sagen, dass IT-Sicherheit oder umgekehrt IT-Kriminalität

das zur Zeit aktuellste und wichtigste Thema darstellt. Viele, wenn nicht alle Unternehmensprozesse sind mittlerweile digitalisiert und die Unternehmen sind abhängig von einer funktionierenden IT-Infrastruktur. Hier ergeben sich immer wieder Angriffsmöglichkeiten von außen wie von innen. Dies ist ebenfalls ein wichtiger Aspekt, auf den ich hinweisen möchte. Angriffe kommen nicht immer nur von außen, sondern auch die eigene Belegschaft, der berühmte Innentäter, kann eine Gefahr darstellen. Für diesen Fall gilt es darauf hinzuweisen, dass zur Abwehr gar nicht so sehr teure, technische Investitionen nötig sind, sondern dass durch gute Führung, durch regelmäßige Information und durch die Sensibilisierung von Mitarbeiterinnen und Mitarbeitern schon viel erreicht werden kann. Es kommt darauf an, klare Regeln im Unternehmen aufzustellen, sich Gedanken darüber zu machen, welche Risiken und Schwachstellen auftauchen können, im Rahmen eines Qualitäts- oder Risikomanagements diese zu kommunizieren und den richtigen Umgang damit durch die Unternehmensleitung vorzuleben.

MITTELSTÄNDISCHE FIRMEN SIND SICH IHRER SICHERHEITSRISIKEN OFT NICHT BEWUSST.

Ulrich Brehmer

Wenn man sich die jährliche Schadenssumme anschaut, dann haben viele Firmen noch kein tiefgehendes Bewusstsein für Unternehmenssicherheit entwickelt. Wie geben sie als Vertreter der ASW damit um?

Generell muss man mit den Summen, die im Umlauf sind, sehr vorsichtig umgehen. Viele basieren auf Schätzungen oder Hochrechnungen von Befragungen. Letztlich sind sie für das einzelne Unternehmen auch so abstrakt, dass Botschaften wie: „Jedes dritte Unternehmen ist betroffen“ oder „bundesweite Schäden von 50 Milliarden € durch Wirtschaftsspionage“ von den Verantwortlichen in den Unternehmen nicht wirklich wahrgenommen werden. Was hilft – und das wünsche ich natürlich niemandem – ist, wenn der Schadensfall tatsächlich eintritt. Dann ist die Sensibilität naturgemäß sehr viel größer. Dann beginnen sich die Unternehmen

darüber Gedanken zu machen, wo ihre schützenswerten Güter tatsächlich sind und wie man diese durch Umstellung von Prozessen, durch personelle Maßnahmen und auch durch den Gedankenaustausch mit anderen Unternehmen absichern kann. Und genau hier bietet die ASW eine Plattform, um mit anderen Firmen ins Gespräch zu kommen, die in einer vergleichbaren Situation sind beziehungsweise waren und um von Experten Lösungswege aufgezeigt zu bekommen. Dies ist, neben dem Zugang zu den Sicherheitsexperten der öffentlichen Seite, der eigentliche Mehrwert der ASW.

Besteht denn bei Unternehmen tatsächlich die Bereitschaft zuzugeben, dass sie einen Sicherheitsfall hatten?

Natürlich liest kein Unternehmen gerne über sich in den Medien, dass es eine Sicherheitslücke gab und dass ein Schadensfall eingetreten ist. Umso wichtiger ist es, die Möglichkeit zu schaffen, sich untereinander auszutauschen, ohne dass man gleich am nächsten Tag in der Zeitung über sich liest.

Wenn der Austausch zwischen Unternehmen und den öffentlichen Behörden funktioniert, warum wird dann zum Beispiel eine Anwaltskanzlei beauftragt, bei der FIFA oder bei VW zu ermitteln? Trauen die Unternehmen das den Sicherheitsbehörden nicht zu?

In der Tat muss die Zusammenarbeit zwischen Unternehmen und Behörden noch deutlich verbessert werden, wenn es um konkrete Vorfälle geht. 2013 haben wir eine Befragung in Norddeutschland durchgeführt und festgestellt, dass im Bereich der IT-Sicherheit weniger als 10 % der Vorkommnisse angezeigt worden sind. Hierfür gibt es verschiedene Ursachen. Das ist zum einen das mangelnde Anzeigeverhalten bei Vorkommnissen im IT-Umfeld, da man unter Umständen nur eine geringe Aufklärungschance sieht. Und zum anderen immer noch der Vorbehalt, dass es gegebenenfalls doch eine Sicherheitslücke gibt und man am nächsten Tag eine entsprechende Schlagzeile in den Medien sieht. Ich erinnere in diesem Zusammenhang nur an den Fall, als der Vorstandsvorsitzende eines DAX-Unter-

nehmens aus seinem Privathaus abgeführt wurde und die Staatsanwaltschaft vorher Medienvertreter informiert hatte, damit diese gute Bilder machen konnten. Daher werden oftmals eigene Ermittlungen vor die öffentlichen Ermittlungen vorgeschaltet. Dennoch ist es natürlich wichtig, das Vertrauen zu den Sicherheitsbehörden zu stärken und wir als Verbände und Kammern wollen unseren Beitrag dazu leisten.

Wenn Sie einen abschließenden Appell an die deutsche Unternehmensgemeinschaft richten könnten, was würden Sie sagen?

Geben Sie dem Thema Schutz der eigenen Interessen, der eigenen Produkte, des betriebsinternen Know-hows und ihrer Mitarbeiter ein ausreichendes Maß an Bedeutung. Definieren Sie die wirklich erfolgsentscheidenden Werte Ihres Unternehmens und ergreifen Sie angemessene Sicherungsmaßnahmen. Dann wird Unternehmenssicherheit kein Kostenfaktor, sondern ein Erfolgsfaktor, der Ihren Unternehmenswert langfristig sicherstellt.

des Unternehmens, vor allem aber in aktuelle Fälle, die das Unternehmen betreffen. Das Personal muss schnell einschätzen können, welche Informationen zu welcher Zeit wohin gelangen und wohin genau nicht. Leitungsvorlagen müssen übersichtlich erstellt und Handlungsempfehlungen umfassend, aber nicht ausufernd sein. All das macht es notwendig, vertrauensvolles Personal in diesen sensiblen Bereich einzusetzen.

Ein Beratungsunternehmen wie die Result Group kann dazu beitragen, vor und während eines Beschäftigungsverhältnisses den Leumund eines (potentiellen) Mitarbeiters zu überprüfen.

Das tun doch auch Personalberatungen oder intern die „Human Resources“-Abteilung.

Das ist richtig, jedoch fehlt es den oben genannten meist am notwendigen Sicherheitshintergrund. Wir befinden uns gerade in einer Zeit, in der sich neben den schon länger vorhandenen Ausbildungsberufen eine akademische Entwicklung zum Sicherheitsmanagement vollzieht. Personen, die den Master im Sicherheitsmanagement haben sind noch nicht so zahlreich und verbreitet. Der typische Leiter Corporate Security hat behördlichen Hintergrund, wie z.B. von Polizei, Geheimdienst oder Militär – mit diesen „Laufbahnen“ und daraus gewonnenen Erfahrungen kann nicht jeder Personalverantwortliche etwas anfangen. Es bedarf also einer Unterstützung bei Auswahl und der „Übersetzung“ von Erfahrungshintergründen und Kompetenzen.

Ist das alles, was Sie beitragen?

Nein, bei Weitem nicht. Neben der formellen Eignung eines Bewerbers oder Mitarbeiters geht es auch um die Sicherheit und Verlässlichkeit der Person. In 2016 hatten wir zwei medienbekannte Beispiele aus den Behörden – das eine war eine Bundestagsabgeordnete, die Ihren Lebenslauf und sogar Abschlüsse gefälscht hatte, der zweite war jüngst ein Mitarbeiter des Ver-

fassungsschutzes, der sich radikalisiert hatte und geheime Informationen weitergab.

Das sind nun bekannt gewordene Fälle, die sicher noch jeder vor Augen hat. In unserer Beratungspraxis treffen wir immer wieder auf Unternehmen, die Bewerber oder aktuelle Mitarbeiter einem sogenannten Pre-Employment-Screening unterziehen. Vor allem wenn es um international zu besetzende Stellen oder Bewerber geht.

Wie geben Sie dabei vor?

Wir unterscheiden bei Pre-Employment-Screenings in drei Stufen, die unterschiedlich intensive Prüfungen nach sich ziehen. Voraussetzung bei allen drei Stufen ist das Einverständnis des Bewerbers und Einsicht in die von ihm eingereichten Unterlagen. Der vorliegende

Rahmen lässt nur eine Kurzbeschreibung zu: Die erste Stufe beinhaltet die Unterlagen und Referenzprüfung. Hatte der Bewerber ein eigenes Gewerbe angemeldet und wo war er die letzten 5 Jahre beschäftigt.

Die zweite Stufe beinhaltet alle Prüfungen der ersten Stufe und darüber hinaus die Überprüfung von Kreditwürdigkeit, Firmenbeteiligungen und die Prüfung von Negativlisten zu Anti Korruption oder Sanktionen. Die dritte Stufe beinhaltet alle Prüfungen der ersten beiden Stufen und erweitert sich auf Reputationsprüfungen vor Ort, Firmenbeteiligungen und Eigentumsverhältnisse – soweit nachvollziehbar und öffentlich zugänglich. Gegebenenfalls werden noch weitergehende Interviews mit dem Kandidaten geführt.

Welche Stufe eines solchen Screenings empfehlen Sie für Stellen in der Corporate Security?

Das lässt sich pauschal nicht beantworten, weil es hier auf die zu besetzende Stelle, den Verantwortungsgrad und die Ausprägung der Vertrauensstellung ankommt. Es muss bedacht werden, was der zukünftige Mitarbeiter alles zu sehen bekommt. Auf der einen Seite sind es die Vorfälle, die tagtäglich auf



INTERVIEW MIT NILS RETKOWSKI:

„DAS PERSONAL DER CORPORATE SECURITY MUSS SCHNELL EINSCHÄTZEN KÖNNEN, WELCHE INFORMATIONEN ZU WELCHER ZEIT WOHIN GELANGEN UND WOHIN GENAU NICHT.“

Was hat ein Beratungsunternehmen für Risiko- und Krisenmanagement zum Auswahlprozess von Mitarbeitern der Corporate Security beizutragen?

Die Funktionen innerhalb der Corporate Security sind sehr sensibel. Die Mitarbeiter erhalten Einblicke in Verfahren und Prozesse, also die „Sicherheitsstruktur“

das Unternehmen zukommen, auf der anderen Seite ist es der Umgang des Unternehmens mit genau diesen Vorkommnissen. Das „Insiderwissen“ ist also geprägt von tiefen Einblicken auch in Schwachstellen und Managementfähigkeiten des Unternehmens.

Das trifft doch aber auf andere Stellen auch zu.

Das stimmt. Doch gerade in der Corporate Security laufen die sensibelsten Probleme auf. Der Vorstand, der bedroht wird; ein Täter, der die Kontaminierung eines Produktes androht; der im Ausland überfallene Mitarbeiter – in den beispielhaft genannten Fällen können Menschenleben gefährdet werden. Es bedarf also einer besonnenen Reaktion und der Vorgehensweise nach zuvor erstellten (Krisen-)Standards. Somit ist nicht nur eine hohe Problemlösefähigkeit, sondern auch eine hohe Stressresistenz vonnöten. All das muss bei der Auswahl von Corporate-Security-Personal betrachtet werden.

Kann man denn jede personelle Entwicklung vorhersagen?

Nein, das schafft ein Pre-Employment Screening nicht. Solch ein Screening gibt jedoch gute Hinweise und offenbart gegebenenfalls schon im Bewerbungs- oder Förderungsprozess Auffälligkeiten des Kandidaten. Nicht immer muss gleich jemand kriminell sein. Doch wie vertrauenswürdig ist jemand, der Lücken in seinem Lebenslauf mit Unwahrheiten deckt?

Können Sie ein Beispiel für Ihre Arbeit geben?

Die Unterlagen des Kandidaten für die Geschäftsführung in einem Land außerhalb Europas waren in Ordnung, Ausbildung und Erfahrung übertrafen die Anforderungen. Trotzdem wollte der Eigentümer, der einen neuen Geschäftsführer suchte, auf Nummer sicher gehen und beauftragte ein Pre-Employment-Screening. Schon bei ersten Prüfungen der Angaben fiel auf, dass diese zum einen beschönigt waren, zum anderen musste die Echtheit einiger Dokumente festgestellt werden. Es kam folgendes zutage – der Kandidat und ein Teil seiner Familienangehörigen hatten Scheinfirmen aufgebaut, die genau die gleichen Geschäftsbereiche abdeckten, die auch unser Mandant bediente. Trotz dieser negativen Hinweise und der

ausgesprochenen Empfehlung zur Nichteinstellung, entschied sich der Unternehmenseigentümer für die Personalie. Alles verlief gut und der Eigentümer war froh über seine Entscheidung. 6 Jahre später kam er jedoch abermals auf die Result Group zu, weil nun Unregelmäßigkeiten festgestellt wurden. Nach Ermittlungen konnte gerichtsverwertbar nachgewiesen werden, dass 6,8 Millionen Euro durch den Geschäftsführer veruntreut wurden. Eine Schadensminderung und optimal die Rückgewinnung des Geldes war überdies Ziel des Auftrages. Das war jedoch nicht alles, aufgrund von Reputationsschäden und gezielter Korruption hatte die Zentrale den Betrieb mit einem Verlust von über 9 Millionen € in diesem Land eingestellt.

Gibt es Bedenkenswertes zum Thema Pre-Employment-Screening?

Es muss dem Bewerber gegenüber darauf hingewiesen werden, dass solch eine Überprüfung durchgeführt wird und die Zustimmung vom Bewerber dazu gegeben werden. Dies signalisiert gleich, dass der Arbeitgeber mit offenen Karten spielt. Gibt der Bewerber sein Einverständnis nicht, wäre zu hinterfragen wieso. Bei der Vorgehensweise ist die Wahrung der Persönlichkeitsrechte eine Selbstverständlichkeit. Hier sei darauf hingewiesen, dass es sich aus zuvor genannten Gründen bei Positionen in der Corporate Security um Stellen handelt, die eine erhöhte Vertraulichkeit an den Mitarbeiter stellen. Als Auswirkung dessen, hat der Arbeitgeber mehr Möglichkeiten, seinen Auswahlprozess zu gestalten. Zum Beispiel in der Beauftragung zu einem Screening. Wir arbeiten im Bereich für Stellen für die Corporate Security eng mit der TOPOS Personalberatung GmbH zusammen. Die Erfahrung in der Sicherheit zum einen und die Kompetenz in der Durchführung von Pre-Employment-Screenings machen diesen Ansatz von TOPOS einzigartig.



INTERVIEW MIT WOLFGANG BENZ:

„**SICHERHEIT** IST NICHT ALLES,
ABER OHNE **SICHERHEIT**
IST ALLES NICHTS.“

Herr Benz, Sie sind seit über 30 Jahren im Themenfeld Sicherheit tätig, zunächst 26 Jahre bei der Hamburger Kriminalpolizei, seit 2010 als Leiter der Unternehmenssicherheit in einem in Hamburg ansässigen Unternehmen. Mit welchen herausragenden Ereignissen sind Sie während dieser Zeit konfrontiert worden?

Fangen wir mit den polizeilichen Ereignissen an. Ich habe eine unglaublich vielfältige Zeit mit bemerkenswerten Kolleginnen und Kollegen erlebt und viel über Menschen und deren Abgründe erfahren, manchmal auch müssen. Hamburg ist aufgrund seiner geografischen Lage mit dem Hafen und seinem weltbekannten Rotlichtviertel ein ausgenommen spannendes Revier für eine Großstadtpolizei.

Im Gedächtnis bleiben neben verschiedenen mehr oder minder umfangreichen Ermittlungsverfahren insbesondere die fast 10 Jahre im Mobilen Einsatzkommando mit spektakulären Kriminalfällen, wie der Erpressung „zum Nachteil“ (wie es im Fachjargon so schön heißt) der Fa. Karstadt, landläufig besser bekannt als der Fall „Dagobert“ oder die Entführung des Hamburger Kaufmanns und Mäzen Jan-Phillip Reemtsma.

Natürlich haben die Einsatzmaßnahmen nach den Anschlägen in New York im September 2001 oder die Planung und Durchführung der Fußball WM 2006 bleibende Eindrücke hinterlassen.

In bester Erinnerung sind aber auch „leise“ Ereignisse, wie der Besuch des damaligen Bundespräsidenten Köhler an „meiner“ Dienststelle oder die Konzeptionierung des Hamburger Weges zur Bekämpfung der Beziehungsgewalt, einem Vorgehen in dem Hamburg lange Zeit Vorreiter in Deutschland gewesen sein dürfte.

Die Herausforderungen in einem Unternehmen sind da anders. Mit meinem Team versuche ich vornehmlich präventiv zu arbeiten und damit für ein sicheres und angenehmes Umfeld für die Kolleginnen und Kollegen im Kerngeschäft zu sorgen.

Inwieweit hat Ihnen Ihre kriminalpolizeiliche Erfahrung in Ihrer jetzigen beruflichen Tätigkeit geholfen?

Wenngleich die Überschrift Sicherheit für beide Aufgaben geeignet ist, sind die Anforderungen doch sehr verschieden. Nach einer so langen Zeit bei der Kriminalpolizei sollte sich eine Fähigkeit zu kriminalistischem Denken entwickelt haben. Das bedeutet, verkürzt Sachverhalte ohne Denkverbote aufzuklären, um daraus Hypothesen zu bilden oder Gefahrenmomente zu identifizieren. Darauf basierend entstehen Lösungsansätze für große und kleine Herausforderungen.

Die Themen Führung UND Vertrauen haben mich geprägt. Gute Führung, das Beschreiben von Leit-

planken und das Vertrauen in die Fertigkeiten und Fähigkeiten der beteiligten Personen sind wichtiger denn je für erfolgreiche Arbeit beim Themenfeld Sicherheit.

Im Laufe der Jahre hat sich neben einer Routine bei Arbeiten in großen Organisationen auch eine Übung im Umgang mit übergeordneten Zielen eingestellt. Das ist nicht nur bei den Maßnahmen nach den Anschlägen von New York, sondern auch u.a. bei der WM 2006 deutlich geworden. Mit einem Moment steht man als Organisation nahezu im weltweiten Interesse und setzt sich natürlich oder zum Glück mit der Frage auseinander, mit welchem Image man wahrgenommen werden möchte. Auch das prägt die Fähigkeit zum taktischen, vorausschauenden Handeln.

Abschließend habe ich gute Erfahrung damit gemacht, genau zu dokumentieren, mit welchem Informationsstand ich welche Entscheidung getroffen habe. Eine Entscheidung von gestern mit den Kenntnissen von heute zu beurteilen ist nicht fair.

Welche Faktoren sind Ihrer Meinung und Erfahrung nach entscheidend für eine erfolgreiche Corporate Security?

Meines Erachtens ist zunächst von überragender Bedeutung, dass das Unternehmen, vertreten durch die Unternehmensleitung, ein klares Zielbild, ein „mission statement“ für die Sicherheitseinheit beschreibt.

Damit einher sollten Überlegungen gehen, wo man eine Sicherheitseinheit „anhängt“. Corporate Security will zum Unternehmenserfolg beitragen, es ist wahrscheinlich ein kleines Rädchen, aber ein wichtiges.

Ich mag die Aussage „Sicherheit ist nicht alles, aber ohne Sicherheit ist alles nichts“. Das Vertrauen muss also da sein, dass die Tätigkeiten einer derartigen Einheit immer an den Zielen des Unternehmens gekoppelt sind und so zum Erfolg beitragen werden.

Und dann benötigt eine Corporate Security vornehmlich eines, nämlich Kompetenz. Welche, entscheidet

in der Regel der Zweck des Unternehmens bzw. die Schwerpunktthemen der Corporate Security.

Die jeweiligen Herausforderungen für Themenverantwortliche, zum Beispiel bei physischer Sicherheit, bei Reisesicherheit oder bei der Einführung eines Informationsmanagementsystems sind so vielfältig, dass die Besetzung einer Einheit mit Generalisten nicht mehr zielführend ist.

Corporate Security muss kommunikativ, zurückhaltend und unaufgeregt sein. Dabei sind Spiele mit der Angst, Drohszenarien und ähnliches denkbar ungeeignet.

Welche Qualifikationen bzw. Skills zeichnen erfolgreiche Leiter bzw. Mitarbeiter in der Corporate Security aus?

Fachliche Qualifikationen sind natürlich unverzichtbar, welche das sein sollten, ergibt sich aus den Anforderungen des Unternehmens. Es sind die „weichen“ Faktoren, die soft skills, die einen Leiter oder Mitarbeiter einer Corporate Security ausmachen sollte. Und da unterscheiden wir uns gar nicht so maßgeblich von unseren Kollegen und Kolleginnen aus den Fachabteilungen. Neben der schon beschriebenen Kommunikationsfähigkeit ist schnelles analytisches Denken und eine gute Entscheidungsfähigkeit essentiell. Ein gehöriges Maß an Belastbarkeit und Einsatzbereitschaft sowie empathische Fähigkeiten runden das Bild ab.

Wie schätzen Sie die Aus- und Fortbildungsmöglichkeiten für zukünftige Mitarbeiter in der Corporate Security ein?

Ich denke, dass wir da noch Luft nach oben haben. Die mir bekannten Bachelorstudiengänge zu Sicherheits- und Risikomanagement und so weiter bilden in der Regel ein solides Fundament.

Danach wird es dann schon enger. Ich begleite, sozusagen seit der Wiege, den derzeit einzigen akkreditierten Masterstudiengang Kriminalistik an der Steinbeis Hochschule in Berlin. Hier bilden wir am Institut

für Kriminalistik neben Polizisten, Rechts- und Staatsanwälten in erster Linie Vertreter aus Unternehmenssicherheiten fort. Neben der Vermittlungsfähigkeit von theoretischem Wissen legen wir bei der Auswahl unserer Referenten besonders Wert auf einen hohen Praxisbezug. Unser Ziel ist es, unsere Absolventen auch für anspruchsvolle Tätigkeiten im Bereich der Corporate Security zu qualifizieren.

Wir brauchen aber mehr, mehr kulturelle Kompetenz, mehr politisch wissenschaftliche Analyse und mehr betriebswirtschaftliches Denken.

Darüber hinaus bin ich ein großer Freund kleiner feiner Angebote. Zielgruppen sind Fachleute aus verschie-

denen Fachrichtungen, die sich zu echten Experten qualifizieren wollen. Ich habe zum Abschluss meiner Tätigkeit bei den Polizei-Spezialeinheiten mehrjährig die Fortbildung geleitet. Bundeslandübergreifend wurden Konzepte erstellt und Fortbildungen durchgeführt, die sich konsequent an den Markterfordernissen orientiert haben.

Nach diesem Prinzip bilden wir bei Steinbeis am Institut für Kriminalistik in Berlin mittlerweile z.B. Experten für Interviews aus und fort. Die Feedbacks der Teilnehmer bzw. der Unternehmen haben uns veranlasst, dieses Vorgehen auch auf andere Themenfelder auszuweiten.

**EINE
ERFOLGREICHE
CORPORATE SECURITY
BRAUCHT EIN
„MISSION STATEMENT“.**

Wolfgang Benz

KONTAKTDATEN

**TOPOS PERSONALBERATUNG GMBH
COMPETENCE CENTER
CORPORATE SECURITY**

Ihre Consultants: Thomas Wilde und Thomas Hölzchen

**Hans-Henny-Jahnn-Weg 35 · 22085 Hamburg
Tel.: +49 (0)40 278499-0 · Fax: +49 (0)40 278499-99
E-Mail: hamburg@topos-consult.de**

IMPRESSUM

Herausgeber:

TOPOS Personalberatung GmbH

V. i. S. d. P.:

Thomas Wilde

Layout:

www.kanebley.de

Bildnachweis:

© Olivier Le Moal / fotolia.com

Auflage:

500

Kontakt:

Hans-Henny-Jahnn-Weg 35, 22085 Hamburg,

Tel.: +49 (0)40 278499-60, Fax: +49 (0)40 278499-99

wilde@topos-consult.de, www.topos-consult.de

TOPOS ●

Hamburg (Head Office)

Hans-Henny-Jahnn-Weg 35

22085 Hamburg

Tel.: +49 (0)40 278499-0

Fax: +49 (0)40 278499-99

E-Mail: hamburg@topos-consult.de

Hannover

Bahnhofstrasse 8

30159 Hannover

Tel: +49 (0)511 93639-454

Fax: +49 (0)511 93639-300

E-Mail: hannover@topos-consult.de

Frankfurt

Bockenheimer Landstraße 17-19

60325 Frankfurt a.M.

Tel.: +49 (0)69 710455-528

Fax: +49 (0)69 710455-450

E-Mail: frankfurt@topos-consult.de

München

Gottfried-Keller-Str. 20

81245 München

Tel.: +49 (0)89 452237-800

Fax: +49 (0)89 452237-829

E-Mail: muenchen@topos-consult.de

Nürnberg

Theodorstraße 9

90489 Nürnberg

Tel.: +49 (0)911 9996994-0

Fax: +49 (0)911 9996994-44

E-Mail: nuernberg@topos-consult.de

Stuttgart

Kreuznacher Straße 60 (Cannstatter Carré)

70372 Stuttgart

Tel.: +49 (0)711 954654-0

Fax: +49 (0)711 954654-6

E-Mail: stuttgart@topos-consult.de