Bedrohungsmanagement in einer komplexen Organisation

Erfahrungen, Strukturen und aktuelle Herausforderungen bei Lufthansa

Ibrahim Karakus, 27.08.2026 – Frag doch mal das Netzwerk

Agenda

Wer ich bin und warum beschäftige ich mich mit dem Thema?

Formen von Bedrohungen und Problemverständnis

Der Lufthansa Ansatz
Die 4 Phasen des BM und vom Hinweis zur verantwortlichen Entscheidung

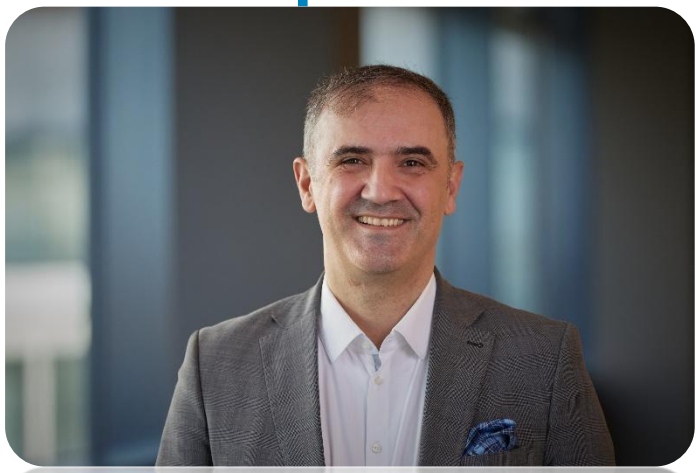
Netzwerk statt Einzelkämpfer
Bedrohungsmanagement ist organisierte Zusammenarbeit.

Wo stehen wir heute?
Vom Einzelthema zu einem systematischen Insider & Threat Management.

Erfahrungen und Herausforderungen
Was wir gelernt haben und was andere mitnehmen können

Dialog: Welche Fragen stellen sich in anderen Organisationen?

Wer spricht heute mit Ihnen?



Ibrahim Karakus

Corporate Security, Insider & Threat Management Lufthansa Group

Seit vielen Jahren mit Unternehmenssicherheit, Prävention, Fallmanagement und Krisenlagen befasst

Zertifizierungen unter anderem in Bedrohungsmanagement, Radikalisierung und extremistischer Gewalt, Stalking sowie Gewalt am Arbeitsplatz

Vernetzung von Unternehmenspraxis, Sicherheitsbehörden und professionellem Bedrohungsmanagement

Vorstandsmitglied Forum Bedrohungsmanagement e.V.

Mitglied und Corporate Security Berater des AETAP Vorstandes

„Mich beschäftigt vor allem eine Frage: Wie können wir handeln, bevor aus einer schwierigen Entwicklung eine ernste Sicherheitslage wird?“

Formen von Bedrohungen

Personenbezogene Bedrohungen

- **Gewalt am Arbeitsplatz:** Androhung oder Ausübung von Gewalt, aggressive Handlungen, Belästigung, körperliche Angriffe und Erpressung
- Stalking: Wiederholte, unerwünschte Verfolgung oder Belästigung mit seelischer oder körperlicher Belastung
- **Radikalisierte Personen und Einzeltäter:** Extremistisch oder religiös motivierte Personen sowie unabhängig Handelnde, die Menschen, das Unternehmen oder Abläufe gefährden können
- **Terrorismus und zielgerichtete Gewalt:** Geplante schwere Gewalttaten, häufig im Zusammenhang mit Radikalisierung oder extremistischer Ideologie

Bedrohungen von Betrieb und Infrastruktur

- **Sabotage:** Vorsätzliche Störung oder Beschädigung von Abläufen, Systemen oder Infrastruktur
- **Cyberangriffe:** Böswillige Kompromittierung oder Störung von IT-Systemen sowie unbefugter Zugriff
- **Straftaten gegen Vermögenswerte:** Diebstahl, Betrug und Einbruch

Insider- und Informationsrisiken

- **Human Intelligence, HUMINT:** Gezielte Gewinnung vertraulicher Informationen durch menschliche Quellen
- **Unzufriedene Mitarbeitende:** Risiken infolge von Frust oder Konflikten, die zu einer Schädigung des Unternehmens führen können

Bewertung des Problems

Gewalt und Bedrohungen im Arbeitsumfeld sind…

- …ein **ethisches Risiko**, da es eine Verantwortung für die Sicherheit der Mitarbeiter gibt…
- …ein **Unternehmensrisiko**, da schwere Gewalttaten wie Amokläufe negative Folgen besitzen, z.B. Einschränkung der Handlungsfähigkeit oder Reputationsschäden…
- …ein **gesetzliches Risiko**, da je nach Staat Schadenersatzansprüche entstehen können, wenn auf Warnsignale der Gewalt nicht reagiert wurde…
- …und ein **Kostenfaktor**, da die Viktimisierung durch Gewalt, Drohungen und Stalking geringere Arbeitsleistung und Arbeitsausfall mit sich bringt

Was Bedrohungsmanagement ist und was nicht!

BM ist

- Präventiv
- verhaltens- und faktenorientiert
- Interdisziplinär
- Dynamisch
- Verhältnismäßig
- Nachvollziehbar dokumentiert

BM ist nicht

- Gedankenlesen
- psychologische Ferndiagnostik
- ein starres Punktesystem
- die Vorhersage einer Tat
- eine Einzelentscheidung aus Security, HR oder Management
- ein Ersatz für Polizei, Medizin, Psychologie, Recht oder Krisenmanagement

Der Lufthansa Ansatz

Die vier Phasen des Bedrohungsmanagements

1

PRÄVENTION

Aufmerksamkeit, Kommunikation, Meldewege

2

VERÄNDERUNG

Belastungen, Auslöser, Gewalt wird eine Option

3

FALLMANAGEMENT

Erkennen, Einschätzen, Entschärfen

4

SUPPORT

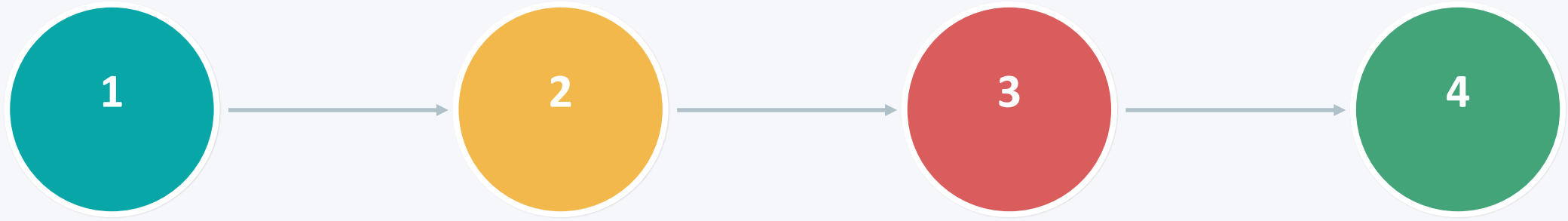
Begleitung, Nachsorge, Lessons Learned

BIG PICTURE

Der Lufthansa Ansatz

Vom Hinweis zur verantwortlichen Entscheidung

Vier wiederkehrende Schritte bilden den professionellen Fallmanagement-Zyklus.



ERKENNEN

Erstkontakt strukturieren
Akutheit und Zuständigkeit klären

EINSCHÄTZEN

Fakten einordnen
Lücken sichtbar machen

ENTSCHÄRFEN

Interdisziplinär planen
Maßnahmen und Rollen klären

EVALUIEREN

Wirkung beobachten
Anpassen und lernen

Wichtig **Bedrohungsmanagement beginnt nicht erst mit einer Drohung und endet nicht mit einer Maßnahme.**

Netzwerk statt Einzelkämpfer

Bedrohungsmanagement ist organisierte Zusammenarbeit.

Fallbezogenes Threat Management Team

Falls erforderlich

Falls erforderlich

Internes Netzwerk

- Psychologischer Dienst
- Medizinischer Dienst
- Psychosozialer Dienst
- Sozialpartner
- Rechtsabteilung
- Operative Sicherheit

Externes Netzwerk

- Sicherheitsbehörden
- Schutzeinrichtungen
- FBM
- Sicherheitsdienstleister
- Krisenberatung

Keine Einzelentscheidung, sondern strukturierte Teamleistung

mit klarer Dokumentation, Rollenklärung und ethischer Reflexion

Wo stehen wir heute?

Governance und Standards

- Einbettung in das Security Management
- definierte Rollen und Verantwortlichkeiten
- strukturierte Fallbearbeitung
- Code of Conduct und Datenschutz

Netzwerk und Fallmanagement

- ausgebildete Threat Manager
- interne und externe Kooperation
- fallbezogene interdisziplinäre Zusammenarbeit
- Erfahrungsaustausch und Community

Vier Handlungsfelder

Awareness und Qualifizierung

- zielgruppenspezifische Trainings
- Web-based Training
- Sensibilisierung von Führungskräften und Mitarbeitenden
- Klarheit über Meldewege

Insider Risk Prävention

- risikobasierte Betrachtung sicherheitskritischer Funktionen
- Kombination mehrerer Sicherheitsmechanismen
- Einbeziehung der Employee Journey
- Weiterentwicklung von Recruiting- und Screening-Prozessen

Erfahrungen und Herausforderungen

Was wir gelernt haben und was andere mitnehmen können

1. Awareness ist das eigentliche Frühwarnsystem
2. Eine Meldung ist noch keine Bewertung
3. Kein Tool (keine KI) ersetzt die fachliche Einordnung
4. Bedrohungsmanagement ist Teamarbeit
5. Prävention braucht Vertrauen
6. Keine Bewertung von Menschen, sondern von Risiken
7. Es gibt keine Einzelmaßnahmen gegen Insider-Risiken

"Bedrohungsmanagement bedeutet nicht, Gefahren vorherzusagen. Es bedeutet, Risiken frühzeitig zu erkennen, professionell einzuschätzen und gemeinsam zu reduzieren."

Ibrahim Karakus

ibrahim.karakus@dlh.de

www.linkedin.com/in/ibrahim-karakus-4a816b1

www.forum-bedrohungsmanagement.de