

Sicherungsanalyse

Hans-Joachim Uth, Berlin

***DECHEMA Weiterbildungskurs „Schutz von
Chemieanlagen gegen kriminelle Angriffe“***

2. – 3. Juni 2005, Frankfurt

Einführung

- Das BMU hat aus Anlass der Terroranschläge vom 11. September 2001 in den USA die SFK um Prüfung der Frage gebeten, welche Konsequenzen aus der neuen Bedrohungssituation für den Bereich der Anlagensicherheit zu ziehen sind.
- Das Ergebnis der Prüfung ist im Bericht SFK-GS-38 niedergelegt.

Anwendungsbereich:

Welche Betriebe sind betroffen ?

- in erster Linie Betriebsbereiche nach der StörfallV mit **erweiterten Pflichten**.
- Betriebsbereiche mit **Grundpflichten** soweit besondere **schutzwürdige Objekte** in der Nachbarschaft vorhanden sind.

Dabei gilt:

In diesen Betriebsbereichen muss eine besondere Gefährdung durch den Eingriff Unbefugter zu besorgen sein.

Definitionen -1

- **Besondere Schutzobjekte** sind Einrichtungen, die zum regelmäßigen Aufenthalt von einer Vielzahl von Menschen vorgesehen sind (Schulen, Versammlungsstätten, Krankenhäuser, Bahnhöfe, etc.).
- **Sicherungsrelevante Anlagen** sind Anlagen in einem Betriebsbereich nach StörfallV, die bei Eingriffen Unbefugter eine ernste Gefahr im Sinne der Störfall-Verordnung für besondere Schutzobjekte hervorrufen können.
- Ein **Unbefugter** ist jede Person, die vorsätzlich Handlungen mit dem Ziel vornimmt, unmittelbar oder mittelbar einen Schaden zu verursachen.

Definitionen -2

- **Sicherung** sind alle Aktivitäten zur Verhinderung von Gefahren, die durch Eingriffe Unbefugter ausgelöst werden können, sowie zur vorbeugenden Begrenzung von Auswirkungen.
- Eine **Sicherungsanalyse** ist die Ermittlung und Bewertung von möglichen Eingriffen Unbefugter und der dadurch möglicherweise ausgelösten Gefahren unter Verwendung von systematischen Methoden.

Ermittlung der Betriebe in denen eine besondere Gefährdung durch den Eingriff Unbefugter besteht

Betroffene Betriebsbereiche

Generell: Betriebsbereiche mit erweiterten Pflichten

Einzelfall: Betriebsbereiche mit Grundpflichten wenn Gefahrenanalyse positiv.

Sicherungsanalyse

Gefahrenanalyse

- Beschreibung der Dennoch-Störfälle
- Besonders schutzwürdigen Objekte
- Auswirkungen der DS bewirken ernste Gefahr bei schutzwürdigen Objekten

Gefährdungsanalyse

- Angreifbarkeit
- Bedeutung der Verfügbarkeit
- Symbolcharakter

Rückkopplung mit **Innen Behörde**

positiv

Immissionsschutz-behörden

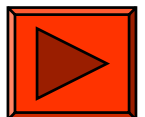
Überprüfung der Betreibermaßnahmen.

Betreibermaßnahmen

- Sicherung der Werksgrenzen
- Sicherung der Anlagen
- Sensibilisierung der Mitarbeiter
- Ergänzung der Sicherheitsberichte
- Alarm- und Gefahrenabwehrpläne

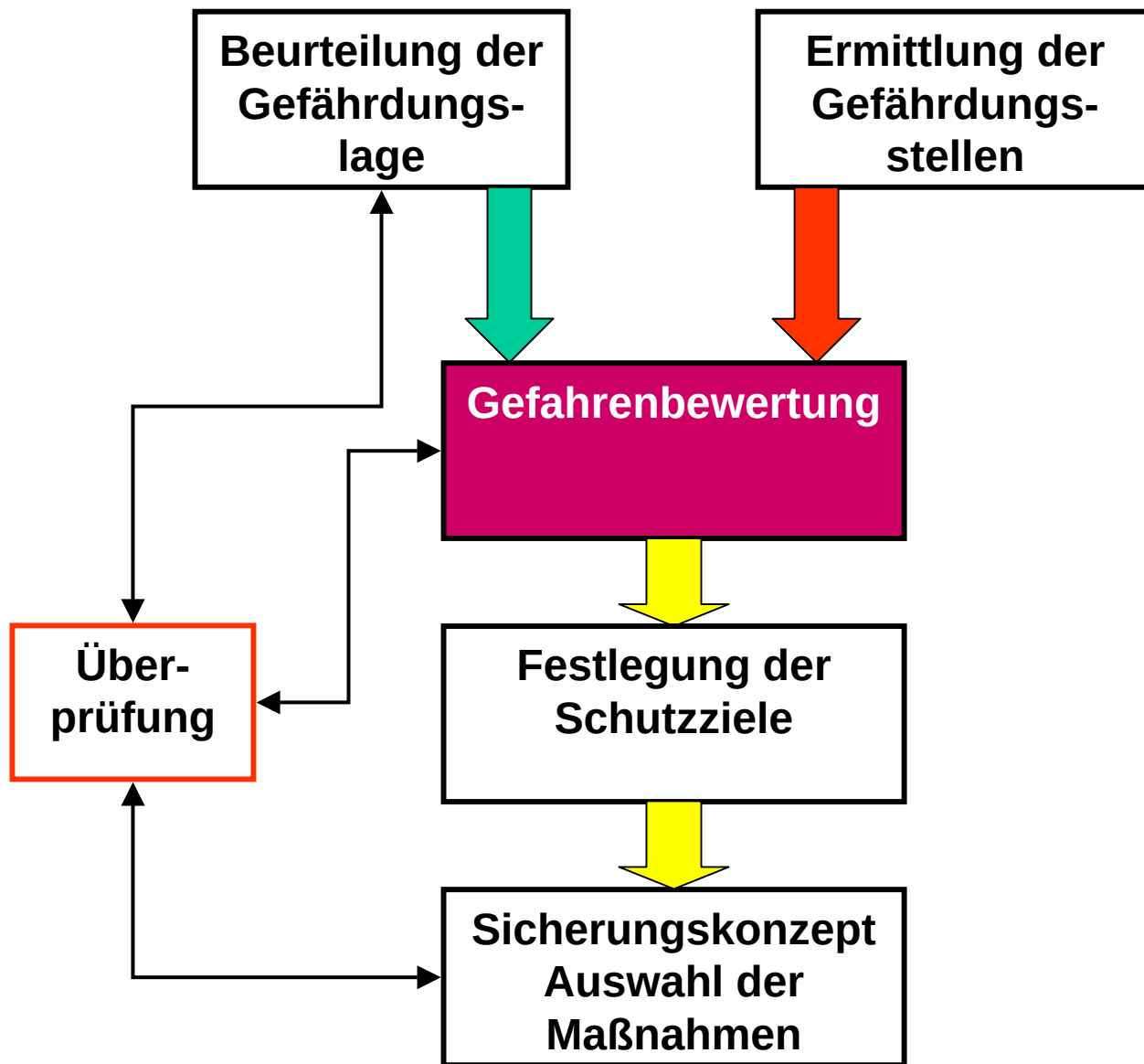
Gefahrenabwehr-behörden

Unverzügliche Anpassung der externen Alarm- und Gefahrenabwehrpläne.

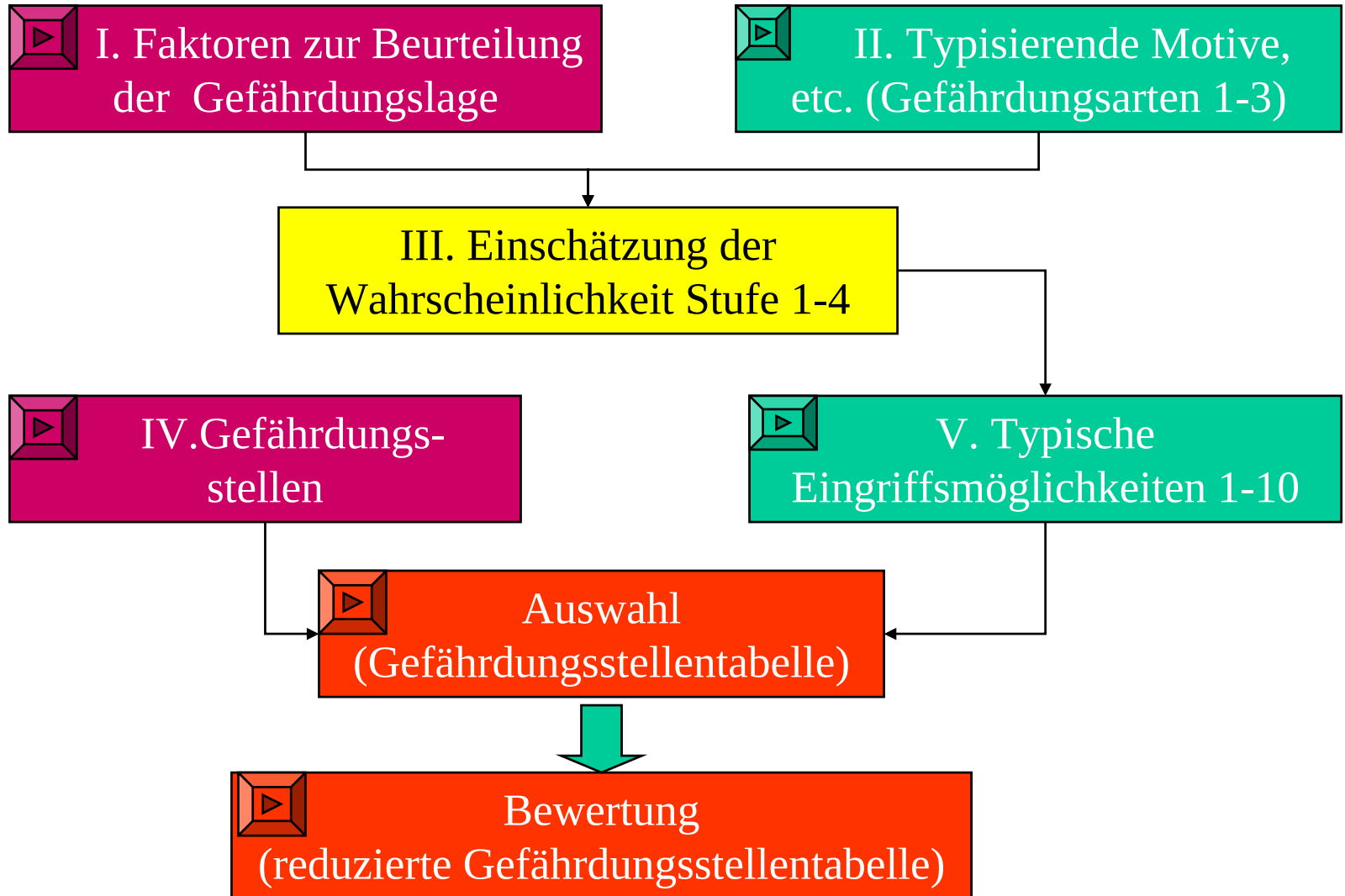


**Die Auswahl der geeigneten
Maßnahmen erfolgt
zweckmäßigerweise gemäß einer
systematischen Sicherheitsanalyse.**

Vorgehensweise bei der Sicherheitsanalyse



Ermittlung des Bedrohungsgrads



Schritt I: Faktoren zur Beurteilung der Gefährdungslage

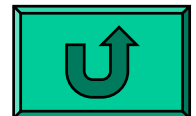
– Allgemeine Informationen–

- allgemeine Sicherheitslage (polizeiliche Kriminalstatistik, Veröffentlichungen der Versicherer, kriminalpolizeiliche und verfassungsschutzmäßige Erkenntnisse der Behörden).
- Zugehörigkeit des Betriebsbereichs zu anderen Unternehmen ((globale) Gefährdungslage des Gesamtunternehmens).
- Bedeutung des Betriebsbereichs für nachgelagerte Produktionen und Dienstleistungen (Schlüsselfunktion).
- Art der Vertriebsverbindungen und Auslandsaktivitäten (Geschäftsverbindungen mit politisch instabilen Ländern).
- örtliche Lage des Betriebsbereichs (benachbarte Betriebsbereiche, Zugänglichkeit, Art und der Umfang der Bebauung).

Schritt I: Faktoren zur Beurteilung der Gefährdungslage

– betriebsspezifische Informationen–

- Art der Produktion, Lagerung von Gefahrstoffen.
- Größe und Zusammensetzung der Belegschaft (Innentäter, Fremdfirmenmitarbeiter, Ausländische Mitarbeiter, Betriebsfremde Personen, Sprachbarrieren).
- Sicherungsmanagement, Unternehmenspolitik (Qualität der Sicherheitsorganisation, Betriebsklima, Festlegung der Sicherungsprozesse).
- Gesellschaftliche Position von Angehörigen der Unternehmensleitung (Aktivitäten in Verbänden oder Parteien).
- bisher festgestellte Kriminalität (Delikte der letzten 5 Jahre, organisierte Kriminalität, Sabotagehandlungen, Brandstiftungen).
- betriebsspezifische Besonderheiten.



Schritt II: Typisierende Gefährdungsarten Typ -1

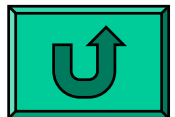
Begleitumstände	Bedingter Vorsatz
Motive	Rache, Frustration
Vorbereitungshandlungen	Ausspähen, Beschaffen von Werkzeugen
Tatmittel	Einfache und schwere Werkzeuge ggf. einfache Brandsätze
Kriminelle Energie	durchschnittlich
Personenkreis	Straftäter aus dem Innen- und Außenbereich
Anmerkungen / Beispiele	Außerbetriebsetzen von Sicherheitseinrichtungen, Eingriffe in Produktionsabläufe, Brandstiftung

Schritt II: Typisierende Gefährdungsarten Typ -2

Begleitumstände	Direkter Vorsatz
Motive	politische Radikalität, Racheakt, Erzielen von Vermögens-/Wettbewerbsvorteilen.
Vorbereitungshandlungen	Erkunden sicherheitsrelevanter Anlagenteile und Schwachstellen, Ausnützen von Lücken bei der Überwachung.
Tatmittel	Einfache und Spezialwerkzeuge, Brandsätze, einfache Sprengmittel (Selbstbau).
Kriminelle Energie	Überdurchschnittlich
Personenkreis	Einzeltäter, Tätergruppen, auch im Rahmen der „organisierten Kriminalität“, radikale politische Gruppen.
Anmerkungen / Beispiele	Brandstiftung/Sprengstoffanschlag, Zerstören von wichtigen Betriebseinrichtungen, Eingriffe in Steuerungsanlagen.

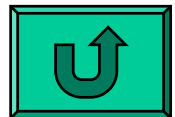
Schritt II: Typisierende Gefährdungsarten Typ -3

Begleitumstände	Massive terroristische Anschläge
Motive	"Fanal setzen", Anarchismus, Herbeiführen gesellschaftlicher Veränderungen mit Gewalt, "Bestrafen" von Unternehmen, glaubensbezogene Motive.
Vorbereitungshandlungen	Logistische Vorbereitungen, Ausspähung, Außerbetriebsetzen von Sicherheitsanlagen.
Tatmittel	Einfaches und schweres Werkzeug, Waffen, Brandsätze, Sprengstoff.
Kriminelle Energie	Außergewöhnlich hoch
Personenkreis	Extremistische und terroristische Einzeltäter und Gruppen.
Anmerkungen / Beispiele	Bewaffneter Überfall, Aufsprengen, Beschuss, in Brand setzen größerer Anlagen, Angriffe auf Werkschutz, Sprengstoffanschläge auf besonders empfindliche Bereiche.



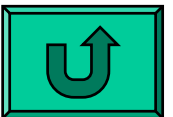
Schritt IV: Typische Gefährdungsstellen

- Behälter, Lagerstellen, Abfüllstationen,
- Steuerzentralen, Schaltwarten, EDV-Anlagen,
- Rohrkanäle, Kabeltrassen, Pumpenhäuser, Ventilgalerien,
- Produktionshallen, Abschnitte,
- Kühlaggregate, Notaggregate aller Art,
- Hochspannungsleitungen und Einspeisestellen,
- Elektroversorgungseinrichtungen,
- Energieversorgungsanlagen aller Art.



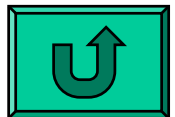
Schritt V: 10 Typische Eingriffsmöglichkeiten

Nr	Bezeichnung	
01	Vorsätzliches Fehlbedienen	
02	Manipulieren	
03	Fahrzeugunfall	
04	Eingriffe mit einfachen Tatmitteln	
05	Eingriffe mit schweren Tatmitteln	
06	Brandstiftung mit einfachen Mitteln	
07	Brandstiftung mit brandfördernden Mitteln	
08	Einsatz von Sprengstoffen	
09	Beschuss	
10	Ereignisse außerhalb der eigentlichen Anlage	



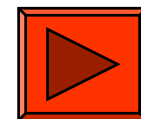
Gefährdungsstellen-Tabelle (Auszug)

Nr.	Einwirkungsmöglichkeit	Gefährdungsstelle 1 Tanklager	Gefährdungsstelle 2 Halle	Gefährdungsstelle 3 Rohrbrücke
01	vorsätzliches Fehlbedienen	Ja	Ja (Während Produktion)	nein
02	Manipulieren	Nein	Nein	nein
03	Fahrzeugverkehr	Ja	Nein	nein
04	Eingriffe mit einfachem Werkzeug	Nein	Ja	nein



Gefahrenbewertung (reduzierte Gefährdungsstellentabelle)

Nr.	Einwirkungs- möglichkeit	Gefährdung sstelle 1 Tanklager	Gefährdung sstelle 2 „Halle“	Gefährdung sstelle 4 „Warte“
01	vorsätzliches Fehlbedienen	ja	ja	_____
02	Manipulieren	_____	_____	ja
04	Eingriffe mit einfachen Tatmitteln	ja	_____	_____
10	Ereignisse außerhalb Anlage	ja (Brand in Gebäude "X")	_____	_____



Vorsätzliches Fehlbedienen (01)

- Schalten/Abschalten von Einrichtungen,
- Auf-/Zudrehen von Rohrleitungsverschlüssen (Schiebern),
- Drehen von Handrädern, Betätigen von Hebeln im Prozessverlauf, usw.

Täterprofil: Das vorsätzliche Fehlbedienen kann durch Mitarbeiter oder Betriebsfremde vorkommen.



Manipulieren (02)

- Fehlprogrammieren von Steuerungen,
- Dejustieren von Messeinrichtungen,
- Unterdrücken von Prozess-, Stör- oder Alarmmeldungen,
- Vorbereitendes Verhindern des Startens von Notaggregaten,
- Ausschalten von Schutzsystemen, usw.

Täterprofil: »Insider« mit genauen Kenntnissen.



Fahrzeugunfall (03)

- Fasseckage durch Gabelstaplerunfall,
- Entgleisen von Kesselwagen,
- Zerstören von Anlagen durch LKW-Aufprall, usw.

Täterprofil: Mitarbeiter und Firmenfremde.



Eingriffe mit einfachen Tatmitteln (04)

- Durchtrennen von Leitungen,
- Zerschlagen von Glasteilen der Anlage (z.B. Füllstandsmesseinrichtungen),
- Festklemmen beweglicher Teile einer Anlage,
- Zumischen nicht erlaubter Stoffe in den Prozess, usw.

Täterprofil: in erster Linie Mitarbeiter.



Eingriffe mit schweren Tatmitteln (05)

- Aufbrechen von Türen und anschließendes Zerstören von Einrichtungen,
- Zerschlagen von Mess- und Steuereinrichtungen,
- Aufschlagen von Behältern und Rohrleitungen mit der Folge größerer Leckagen, usw.

Täterprofil: Alle



Brandstiftung mit einfachen Mitteln (06)

- Anzünden von brennbaren Flüssigkeiten aus dem verfahrenstechnischen Ablauf,
- In Brand Setzen von Lagerstellen mit der Folge des Freisetzens gefährlicher Stoffe,
- In Brand Setzen von peripheren Räumen oder Einrichtungen mit Auswirkungen auf wichtige Anlagenteile, usw.



Brandstiftung mit brandfördernden Mitteln (07)

- Ausgießen und Anzünden von brennbaren Flüssigkeiten (z.B. Benzin),
- Werfen von sogenannten »Molotow-Cocktails« (z.B. auch durch Fenster),
- Anbringen professioneller Brandsätze mit Zeit- oder Fernzündeinrichtungen.

Täterprofil: Die Anschläge setzen eine hohe kriminelle Energie voraus.



Einsatz von Sprengstoffen (08)

- Anordnen einer »Feuerlöscher-Bombe« (Selbstlaborat) in empfindlichen Anlagenteilen oder wahrscheinlicher an der Gebäudeperipherie,
- Aufsprengen von Behältern und Rohrleitungen,
- Wegsprengen von tragenden Bauteilen mit der Folge des Umstürzens von Behältern,
- Zerstören von Anlageteilen, usw.

Täterprofil: In der Regel Fremdeinwirkung mit radikalem Hintergrund.



Beschuss (09)

- Verursachen von Leckagen in freistellenden Behältern oder in Rohrleitungen,
- Ausschalten von Mess- und Überwachungseinrichtungen aus der Entfernung,
- Ausschalten von Versorgungseinrichtungen aus der Entfernung.

Täterprofil: terroristischer Täter von außerhalb.



Ereignisse außerhalb der eigentlichen Anlage (10)

- im Brandfall das Übergreifen eines Feuers von benachbarten Einrichtungen,
- der Flug von Trümmern nach einer Explosion in benachbarten Einrichtungen,
- der Ausfall von Versorgungseinrichtungen durch Katastrophenereignisse außerhalb der Anlage, usw.



Sicherungsziele

Sicherungsmaßnahmen können nur dann sinnvoll geplant werden, wenn klare Zielvorgaben über das bestehen, was sie bewirken sollen.

Beispiele

- Der Zugriff auf die Steuerungseinrichtungen nur durch autorisiertes Personal.
- Sicherheitsrelevante Schalteinrichtungen werden überwacht.
- Der Gefahrenbereich ist vom übrigen Betriebsgebäude abgetrennt.
- Das Eindringen in das Lagergebäude nach Dienstende ist durch Barrieren erschwert.

Beschreibung der Sicherungsmaßnahmen / Sicherungskonzept

- Standort und Lage.
- Äußere Umschließung.
- Zugangs-/Zufahrtskontrolle durch Pforten.
- Sicherung gefährdeter Bereiche (Abwehr unbefugter Personen).
- Organisatorische Maßnahmen (Ausweiswesen, Zugangserlaubnis, Schlüsselwesen, Personalkontrolle bei Fremdpersonal).
- Sicherungsorganisation (Werkschutz).
- Melde-, Überwachungs- und Kommunikationssysteme.

Dokumentation

Die Analyse und die daraus abgeleiteten Maßnahmen sollten dokumentiert werden. Diese Dokumentation ist jedoch in besonderem Maße **geheimhaltungsbedürftig** und sollte auch innerhalb des Unternehmens nur einem beschränkten Kreis von Mitarbeitern zugänglich sein. Aus Unterlagen, die allen Mitarbeitern und der Öffentlichkeit zur Verfügung stehen, sollte jedoch schlüssig hervorgehen, dass der Betreiber die notwendigen Maßnahmen zur Sicherung des Betriebsbereichs und der Anlagen gegen Eingriffe Unbefugter getroffen hat.

Sicherung von Industrieanlagen gegen Eingriffe Unbefugter

A1 Sicherheitsüberprüfung von Mitarbeitern

A2 Umgang mit und der Prävention von vorsätzlich schädigendem Mitarbeiterverhalten

B Einschränkung der Zugänglichkeit von Unterlagen aus Gründen der öffentlichen Sicherheit

FN: EcoTeam, Trier, und Dr. U. Neuser, Berlin

Bericht UFOPLAN-202 48 376

www.umweltbundesamt.de/anlagen

A 1 Sicherheitsüberprüfung von Mitarbeitern

- Untersuchung der Möglichkeit der „Sicherheitsüberprüfung von Mitarbeitern“ als Schutzmaßnahme gegen potenzielle Innentäter auf der Grundlage des Sicherheitsüberprüfungsgesetzes. (Vergleich mit Luftverkehrs- und Atomrecht)
- Vorschlag zur Vorgehensweise zur Identifizierung des überprüfungspflichtigen Personenkreises.

A2 Umgang mit und der Prävention von vorsätzlich schädigendem Mitarbeiterverhalten

- Untersuchung der Motive und Gründe der Motiventstehung bei Innentäter, die aus Unzufriedenheit, Verärgerung über Arbeitgeber, Vorgesetzte oder Arbeitsbedingungen dem Unternehmen Schaden zufügen wollen und damit Störfälle riskieren.
- Entwicklung und Bewertung von Strategien zur Vermeidung der Entstehung schädigender Motive.
- Leitfaden für die betriebliche Praxis zur Minderung schädigenden Mitarbeiterverhaltens in Organisationen.

B **Einschränkung der Zugänglichkeit von Unterlagen aus Gründen der öffentlichen Sicherheit**

- Klärung rechtlicher Voraussetzungen für den Geheimnisschutz von Unterlagen (insbesondere des Sicherheitsberichtes) aus Gründen der öffentlichen Sicherheit.
- Entwicklung von Entscheidungskriterien für die Einschränkung der Informationsrechte der Öffentlichkeit auf der Grundlage von BImSchG und UIG (einschließlich der Verordnungen)
- Überprüfung der Kriterien an zwei Beispielen.

Informationsquellen SVA (Auswahl)

- Deutsche Empfehlungen: www.umweltbundesamt.de/anlagen
- US Empfehlungen:
<http://yosemite.epa.gov/oswer/ceppoweb.nsf/content/links.htm?openDocument#security>
- Guideline of CCPS: <http://www.aiche.org/industry/ccps/sva/index.htm>
- US Ministry of justice: <http://www.ncjrs.org/pdffiles1/nij/195171.pdf>
- Responsible care program:
<http://www.responsiblecaretoolkit.com/security.asp>
- SOCMA: Chemical Site SVA Model & Manual:
<http://www.socma.com/products/VulnerabilityAnalysis.htm>
- OECD Working Group on Chemical Accidents: Report of the Workshop on Communication related to Chemical Releases Caused by Deliberate Acts, Rome, Italy, 25-27 June 2003 No. 12, ENV/JM/MONO(2004)3