

Betriebsspionage und Geheimnisschutz

Sicherheitsrisiken und Werkschutz im Unternehmensalltag

**Technologieschutz im Kontext:
Carl Heymanns Patenttage Osnabrück
2 Juni 2017**

Dr. Mirko Vianello
Rechtsanwalt (Syndikusrechtsanwalt)
Senior Legal Counsel - Global Intellectual Property (G-FLP/T)

Agenda

1. Unternehmensschutz
2. Werk- und Informationsschutz
3. Typische Gefahren für den Verlust von Betriebs- und Geschäftsgeheimnissen
4. Neue Herausforderungen an die Unternehmerpraxis aufgrund der Richtlinie (EU) 2016/943 über den Schutz vertraulichen Know-hows und vertraulicher Geschäftsinformationen (Geschäftsgeheimnisse)

Bei der Abwehr von **Betriebsspionage / Wirtschaftsspionage** geht um den Schutz von „**Geschäftsgeheimnissen**“.

„Geschäftsgeheimnisse“ i.w.S. sind **Informationen**, technischer oder nicht technischer Natur, die bestimmte Kriterien erfüllen.

Know-how und vertrauliche Geschäftsinformationen werden vor **rechtswidrigem Erwerb** (Spionage) sowie **rechtswidriger Nutzung und Offenlegung** (Verrat) geschützt.

Der Ansatz für den Unternehmensschutz sollte

- **weltweit**
- **allumfassend**
- **dezentral**
- **unternehmensintern**

sein.



Permanente Überwachung rund um die Uhr.

Unternehmensschutz



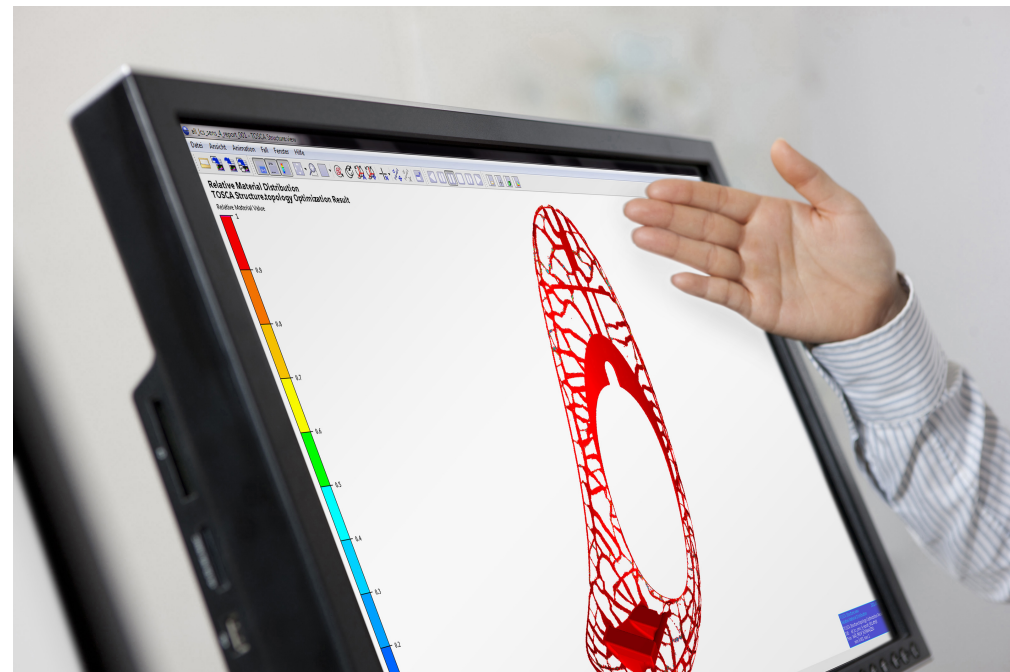
Werkschutz wird als **physische Sicherheit** (Objektschutz) durch Kombination von Personal und Technik verstanden:

- Zugangskontrollen
- Überwachungs- und Alarmanlagen
- Durchsetzungs- und Verfolgungsmaßnahmen



Informationsschutz zielt mehr auf den Schutz der **digital** gespeicherten sensiblen **Firmendaten** ab.

- Schutz vor externen Angriffen (Industriespionage)
- Schutz vor Datenverlust
- Gesamtheitliches Datenschutzkonzept



Mindestanforderungen mit ganz konkrete Handlungsanleitungen für den Umgang mit sensiblen Informationen:

Fünf Bausteine:

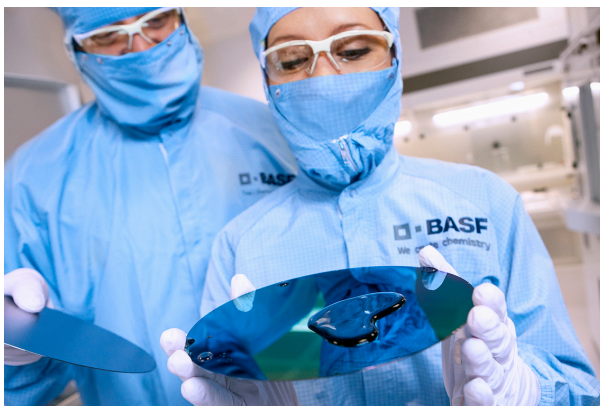
1. Informationsschutz ist Teil der täglichen Arbeit!
2. Nur Berechtigte haben Zugriff auf und Zutritt zu Informationen!
3. Informationsträger werden sicher aufbewahrt, gesichert, transportiert und qualifiziert entsorgt!
4. Informationsschutz auch auf Reisen und unterwegs beachten!
5. Informationstechnologien sicher nutzen!

Typische Gefahren für den Verlust von Betriebs- und Geschäftsgeheimnissen



© BASF SE

Ausgeschiedene



© BASF SE

Nachlässigkeiten



© BASF SE

Diebstahl

Neue Herausforderungen an die Unternehmerpraxis

Durch die Richtlinie (EU) 2016/943 stellen sich vor allem folgende neue Herausforderungen an die Unternehmenspraxis:

1. Identifikation von Geschäftsgeheimnissen?
2. Klassifizierung von Geschäftsgeheimnissen?
3. Markierung von Geschäftsgeheimnissen?
4. Bedarf es einer speziellen „Trade Secret Policy“ und/oder genügen „Richtlinien zum Informationsschutz“?
5. Bedarf es eines speziellen Teams innerhalb des Unternehmens, das sich unabhängig von einem Informationsschutzteam mit der Überwachung des Schutzes von Geschäftsgeheimnissen befasst?



We create chemistry