

Anders als die Polizei bzw. die Staatsanwaltschaft unterliegen wir nicht dem Strafverfolgungszwang, so dass den betroffenen Unternehmen ein **Höchstmaß an Vertraulichkeit** zugesichert werden kann.

### : Kontakt

Vielleicht hat diese Information dazu geführt, dass Sie einen (Einbruch-) Diebstahl in Ihrem Unternehmen nun in einem anderen Licht betrachten, vielleicht haben Sie auch allgemeine Fragen zum Thema Wirtschaftsspionage oder zu den Möglichkeiten, ungewolltem Know-how-Abfluss vorzubeugen. Sprechen Sie uns an, arbeiten Sie mit uns zusammen, wir können beraten und helfen!

### : Ihre Ansprechpartner

Abteilung 6: Tel: 0211 / 871 2821  
E-Mail: abteilung-vi@im.nrw.de

Werner Backes: Tel: 0211 / 871 2916  
E-Mail: werner.backes@im.nrw.de

Jürgen Helbig Tel: 0211 / 871 2737  
E-Mail: juergen.helbig@im.nrw.de

Wilfried Karden Tel: 0211 / 871 2334  
E-Mail: wilfried.karden@im.nrw.de

Reinhard Vesper: Tel: 0211 / 871 2885  
E-Mail: reinhard.vesper@im.nrw.de

Verfassungsschutz Tel: 0211 / 871 2821  
[www.im.nrw.de/wirtschaftsspionage](http://www.im.nrw.de/wirtschaftsspionage)

[www.im.nrw.de](http://www.im.nrw.de) : Wirtschaftsspionage

# Wirtschaftsspionage durch Diebstahl und Einbruchdiebstahl

Aktuelle Informationen für die Wirtschaft



: im Internet unter [www.im.nrw.de/wirtschaftsspionage](http://www.im.nrw.de/wirtschaftsspionage)



Herausgeber

Innenministerium des Landes  
Nordrhein-Westfalen  
Abteilung Verfassungsschutz  
Postfach 10 30 13  
40021 Düsseldorf  
Haroldstraße 5  
40213 Düsseldorf  
Telefon: 0211/871 2821  
Telefax: 0211/871 2980  
[bestellung.verfassungsschutz@im.nrw.de](mailto:bestellung.verfassungsschutz@im.nrw.de)  
<http://www.im.nrw.de/verfassungsschutz>



*Wirtschaftsspionage ist die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Betrieben.*

*Von **Konkurrenzausspähung** oder auch **Industriespionage** spricht man dagegen bei der Ausforschung, die ein (konkurrierendes) Unternehmen gegen ein anderes betreibt.*

### **(Einbruch-) Diebstahl und Wirtschaftsspionage?**

In Ihr Unternehmen wurde eingebrochen? Haben Sie schon einmal daran gedacht, dass es der Dieb nicht auf die entwendeten Gegenstände abgesehen haben könnte, sondern auf Ihr Know-how?

Aus den vielfältigen Kontakten mit nordrhein-westfälischen Unternehmen und individuellen Beratungsgesprächen hat die Spionageabwehr NRW einen guten Überblick über die Methoden, mit denen fremde Nachrichtendienste versuchen, das Know-how deutscher Unternehmen anzupapfen: Einbruch und Diebstahl gehören dazu. Mit diesem Flyer möchten wir Ihren Blick schärfen, denn der Diebstahl wird in den meisten Fällen nicht als Spionageversuch erkannt.

### **Aktuelle Beispiele**

- 1. In einem mehrstöckigen Firmengebäude drangen die Täter gezielt in die achte Etage ein und entwendeten dort ausgewählte Datenträger. Hierbei ließen sie andere lohnende Beutestücke wie Flachbildschirme, Notebooks, Bargeld o. ä. außer Acht.*
- 2. Die Täter brachen in ein Firmengebäude ein und begaben sich – wie an den Spuren erkennbar war – auf direktem Wege in den IT-Bereich, wo versucht wurde, die Firmendaten von dem Server herunterzuladen.*
- 3. Eine Delegation ließ sich in einem Unternehmen eine neue Anlage vorführen. Die Steuerung des Verfahrens erfolgte über ein älteres Notebook. Dies bewahrte der zuständige Ingenieur in seinem Büro im Schreibtisch auf. Die Täter drangen wenige Tage nach der Präsentation in das Gebäude ein und entwendeten das ältere Notebook aus dem Schreibtisch. Hierbei ließen sie ein neues Notebook samt Netzgerät außer Acht, das auf dem Schreibtisch stand.*

In allen Fällen wurde zunächst nur wegen Einbruch oder Einbruchdiebstahls ermittelt und erst nach einer Sensibilisierung durch die Spionageabwehr die tatsächliche Zielrichtung – der Angriff auf das Firmen-Know-how – erkannt.

Wenn also bei einem Einbruch einer der folgenden Punkte zutrifft, raten wir den betroffenen Unternehmen dringend, auch einen Know-how-Diebstahl in Betracht zu ziehen und die Spionageabwehr NRW zu kontaktieren:

- es besteht der Verdacht eines Zugriffs auf
  - die IT-Systeme
  - auf Auftrags/Kalkulationsunterlagen,
  - auf Prototypen, Modelle oder
  - auf sensibles Firmen-Know-how;
- es wurden nur bestimmte PC, Festplatten, Datenspeicher oder sonstige Informationsträger – auf denen sich wichtiges Firmen Know-how befand – entwendet und hierbei andere zugängliche Wertgegenstände nicht beachtet.

Die Beteiligung fremder Nachrichtendienste an solchen Sachverhalten ist zwar oft schwierig zu belegen, vor allem dann, wenn bereits einige Zeit seit der Tat vergangen ist. Aber gerade deshalb ist es wichtig, die Spionageabwehr so früh wie möglich zu informieren. Denn häufig sind an diesen Straftaten auch **Innentäter** beteiligt, so dass weitere Verluste von sensiblem Firmen-Know-how zu befürchten sind.