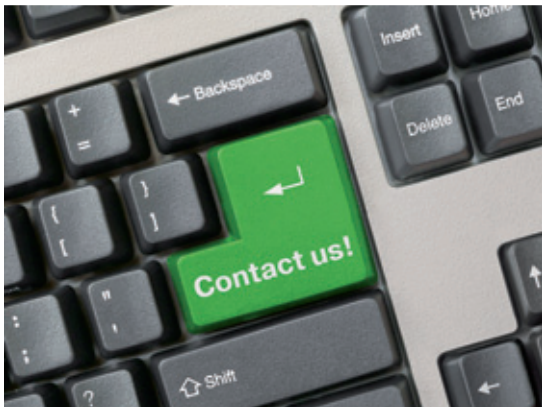


Stellen Sie sich im Schadenfall u.a. folgende Fragen:

- Ist schützenswertes Firmenwissen entwendet worden?
- Ergeben sich für die Täter weitere Zutritts- und Zugriffsmöglichkeiten?
- Bestehen Anhaltspunkte, die auf Insiderwissen oder auf einen Innentäter hinweisen?
- Gibt es Hinweise auf Manipulation an technischen Geräten Ihres Unternehmens?
- Gibt es einen auffälligen Zusammenhang zwischen dem Zeitpunkt des Diebstahls und einem firmenrelevanten Ereignis?

Sprechen Sie uns an und vereinbaren Sie einen Termin für ein vertrauliches Sensibilisierungsgespräch.



Ihre Ansprechpartner

www.verfassungsschutz.de
www.verfassungsschutz-bw.de
www.verfassungsschutz.bayern.de
www.verfassungsschutz-berlin.de
www.verfassungsschutz.brandenburg.de
www.verfassungsschutz.bremen.de
www.hamburg.de/verfassungsschutz
www.verfassungsschutz.hessen.de
www.verfassungsschutz-mv.de
www.verfassungsschutz.niedersachsen.de
www.mik.nrw.de/verfassungsschutz
www.verfassungsschutz.rlp.de
www.saarland.de/verfassungsschutz.htm
www.verfassungsschutz.sachsen.de
www.mi.sachsen-anhalt.de/verfassungsschutz
www.verfassungsschutz.schleswig-holstein.de
www.thueringen.de/de/verfassungsschutz

Impressum: Bundesamt für Verfassungsschutz
für die Verfassungsschutzbehörden
in Bund und Ländern

Bilder: Fotolia

Druck: INFOX GmbH&Co.
Informationslogistik KG, Troisdorf

Stand: Dezember 2011



Wirtschaftsspionage durch Diebstahl und Einbruchdiebstahl

(Einbruch-) Diebstahl und Wirtschaftsspionage?

In Ihr Unternehmen wurde eingebrochen? Wurden Mitarbeiter in Zusammenhang mit ihrer beruflichen Tätigkeit bestohlen? Haben Sie schon einmal daran gedacht, dass das Ziel nicht die entwendeten Gegenstände waren, sondern Ihr Know-how?



Die Verfassungsschutzbehörden haben Erkenntnisse über Methoden, mit denen fremde Nachrichtendienste oder Konkurrenten versuchen, an das Know-how deutscher Unternehmen zu gelangen. Einbruch und Diebstahl gehören dazu.

Unsere Sensibilisierungsgespräche mit Unternehmen bestätigen, dass diese Delikte häufig nicht als spionagerelevant erkannt werden.

Fallvarianten

- In einem mehrstöckigen Firmengebäude drangen die Täter gezielt in die achte Etage ein und entwendeten dort die Festplatten aus mehreren Laptops. Hierbei ließen sie andere lohnende Beutestücke, wie die Laptops selbst, Flachbildschirme und Bargeld außer Acht.
- In einem anderen Fall brachen die Täter in ein Firmengebäude ein und begaben sich – wie anhand der Spuren erkennbar – auf direktem Wege in den IT-Bereich, wo versucht wurde, Firmendaten vom Server herunterzuladen.
- Auf Messen, Flughäfen und Bahnhöfen oder aus Geschäftsfahrzeugen werden immer öfter Laptops, Smartphones sowie Firmenunterlagen entwendet. Nicht selten geht dabei wertvolles Know-how von Unternehmen verloren.
- Heimtückisch sind besonders die Fälle, in denen augenscheinlich nichts entwendet wurde. Werden lediglich Einbruchspuren festgestellt, besteht die Möglichkeit, dass entweder Abhörtechnik wie Wanzen, Kameras und Trojaner eingebracht oder unerkannt Daten oder Kopien mitgenommen wurden.

Erfahrungswerte

In der Regel wurde in solchen Fällen zunächst nur wegen Diebstahl oder Einbruchdiebstahl ermittelt. Erst nach einer Sensibilisierung durch die Verfassungsschutzbehörden zeigte sich die tatsächliche Zielrichtung: der Angriff auf das Firmen-Know-how.



Die Beteiligung fremder Nachrichtendienste an solchen Sachverhalten ist oft schwierig nachzuweisen, vor allem, wenn die Tat bereits einige Zeit zurück liegt. Gerade deshalb ist es wichtig, die Verfassungsschutzbehörden so früh wie möglich zu informieren.

Auch im Hinblick auf mögliche Innentäter ist es wichtig, schnell zu reagieren, um weitere Verluste von sensiblem Firmen-Know-how zu verhindern.