Welches sind die nächsten Schritte?

Bewusstsein schaffen – Verhalten ändern.

Mit diesem Flyer wollen wir einen ersten Anstoß liefern, um Sie mit dem wichtigen Thema Informationsschutz vertraut zu machen. Nun geht es darum, das Bewusstsein in Ihrem Unternehmen zu schärfen und den Schutz von Informationen konsequent im Arbeitsalltag zu verankern.

Eine ausführlichere Checkliste zum Informationsschutz steht Ihnen auf der Internetseite für Kontraktoren zur Verfügung.

Impressum:

BASF SE
Corporate Security
Informationsschutz BASF-Gruppe
information.protection@basf.com

IPMR-9001D
Rev. 2010-07

Corporate Security

Auf Ihren Beitrag kommt es an.

Informationsschutz bei der Zusammenarbeit mit der BASF.

Corporate Security
Informationsschutz BASF-Gruppe

BASF
The Chemical Company

Warum Informationsschutz?

Im Alltag liegt das Risiko.

Der Abfluss vertraulicher Informationen aus Unternehmen richtet nach Expertenschätzungen jährlich Milliardenschäden an. Doch oftmals geht es hier gar nicht um spektakuläre Fälle von Wirtschaftsspionage, sondern um die Folgen kleiner Unachtsamkeiten im ganz normalen Arbeitsalltag. Ein versehentlich liegengelassenes Schriftstück. Ein Virus, freigesetzt durch einen gedankenlosen Download. Ein öffentlich geführtes Telefonat mit vertraulichem Inhalt ...

Diese Risikoquellen existieren überall in unserem Arbeitsalltag. Als Partner, Dienstleister oder Zulieferer der BASF haben Sie ebenfalls immer wieder mit schützenswerten Informationen zu tun.

Deshalb ist es von entscheidender Bedeutung, dass auch Sie geeignete Vorkehrungen zum Informationsschutz treffen. Ganz wichtig dabei: Es handelt sich nicht so sehr um aufwändige und kostenintensive Maßnahmen – sondern vielmehr um eine generelle Änderung des Bewusstseins und des Verhaltens im Umgang mit schützenswerten Informationen.

Auf den folgenden Seiten wollen wir Ihnen einen ersten Überblick über die Bereiche geben, in denen Sie einen entscheidenden Beitrag zum gemeinsamen Informationsschutz leisten können.

Eine Frage der Einstellung.

Wirksamer Informationsschutz ist kein Zauberwerk. Im Gegenteil: Es genügt bereits eine Reihe gezielter Maßnahmen, die Sie ohne viel Aufwand ergreifen können, um Ihr Informationsschutz-Niveau deutlich zu erhöhen. Verschaffen Sie sich anhand der folgenden, knappen Übersicht einen ersten Eindruck vom Status quo in Ihrem Unternehmen.

Wirtschaftsspionage in Zahlen.

Die Delikte im Bereich der Informationsbeschaffung nehmen seit Jahren permanent zu. Es zeigt sich, dass dabei über 80 % der Vorfälle von Mitarbeitern und nur 20 % durch die Technik verursacht werden. Hier einige Zahlen, die Anlass zu höchster Wachsamkeit geben.

- **Jedes fünfte** deutsche Unternehmen ist bereits Opfer von Wirtschaftsspionage geworden.
- **Ca. 2,8 Milliarden Euro** betrug 2006 allein in Deutschland der jährliche Schaden durch unerwünschten Informationsabfluss. Die Dunkelziffer ist dabei viel höher und beträgt nach einer Schätzung des Bundesinnenministeriums in Deutschland ca. 20 Milliarden Euro jährlich.
- **Um etwa 10 %** jährlich steigen die Fälle von Industriespionage.
- **Ca. 15 %** der Delikte werden in Form von Hacking-Angriffen begangen.

Quellen: Studie Industriespionage, hg. v. Handelsblatt, Büro für Angewandte Kriminologie Hamburg und Corporate Trust (2007); Handelsblatt, 07.12.2006, Europäische Kommission.

Was müssen Sie beachten?

Grundlegende Verhaltensweisen.

- Haben Sie den Kreis von Berechtigten festgelegt, der Zugang zu schützenswerten Informationen hat?
- Wurden diese Berechtigten zur Vertraulichkeit verpflichtet und in Sachen Informationsschutz unterwiesen?
- Wird die Durchführung eingeführter Maßnahmen regelmäßig kontrolliert und dokumentiert?
- Halten Sie im Umgang mit personenbezogenen Daten die gesetzlichen Datenschutzbestimmungen ein?

Was müssen Sie beachten?

Schutz vor unberechtigtem Zugriff auf Informationen.

- Haben tatsächlich nur Berechtigte Zugang zu Informationen – und wie werden diese Zugriffsrechte geregelt?
- Welche Schutzmaßnahmen treffen Sie bei Abwesenheit der Berechtigten?
- Gibt es besonders schützenswerte Bereiche in Ihrem Unternehmen? Und wie sind sie gesichert?
- Setzen Sie Passwörter ein – und sind diese ausreichend sicher?
- Wie sicher sind Informationen in hausinternen Postfächern und auf Datenträgern?
- Wie sicher ist die Übermittlung von Informationen via E-Mail, Telefon, Telefax, Videokonferenzen etc.?
- Wie ist in Ihrem Unternehmen der Umgang mit Druckern und Faxgeräten geregelt?
- Führen Sie Besprechungen stets so durch, dass ihr Inhalt nicht an Dritte gelangen kann?

Was müssen Sie beachten?

Qualifizierte Entsorgung von Informationen.

- Erfolgt das Entsorgen von Informationen wirklich sicher? Welche Shredder benutzen Sie?
- Sind Sie in der Lage, Informationen auf Datenträgern vollständig und sicher zu löschen?

Informationsschutz auf Reisen und in der Öffentlichkeit.

- Nehmen Sie tatsächlich immer nur zwingend notwendige Informationen auf Reisen mit?
- Sind Akten oder Laptops unterwegs immer beaufsichtigt sowie gegen Wegnahme und Einblick Dritter gesichert?
- Wie stellen Sie sicher, dass Unberechtigte Ihre Gespräche oder Telefonate nicht mithören können?