

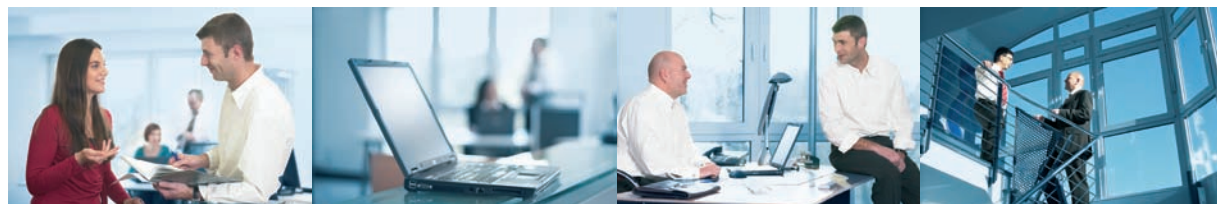
IT-RISIKOMANAGEMENT

**Egal was passiert, meine IT läuft
und läuft und läuft.**



Wir machen Ihre IT.

Sicherheit ist Chefsache.



Jede IT birgt Risiken in sich. Sie leistet Hervorragendes für Unternehmen. Fällt sie aber aus, können Firmen in schwere Bedrängnis kommen. Da reicht möglicherweise schon ein ganz normaler Stromausfall. Wichtig ist deshalb ein durchdachtes IT-Risikomanagement, damit in der Firma jeder weiß, was im Fall der Fälle zu tun ist und der Geschäftsbetrieb sicher weiterlaufen kann.

Gesetze und Compliance-Richtlinien verpflichten heute alle Unternehmen zur Umsetzung eines solchen transparenten IT-Risikomanagement-Systems. Aber gerade für kleine und mittelständische Unternehmen ist das eine große Herausforderung.

Der richtige Partner. Für die beste Lösung.

Verlassen Sie sich beim Thema IT-Risikomanagement auf ausgewiesene Experten. Dank unserer langjährigen Erfahrung können wir sehr schnell feststellen, wo bei Ihrer IT mögliche Schwachstellen liegen. Dazu definieren wir den Ist-Zustand Ihrer Systeme, führen fortlaufend Risikoanalysen aus und erstellen detaillierte Sicherheitsnachweise. Alles mit dem Ziel, die Sicherheit und Verfügbarkeit Ihrer IT im täglichen Betrieb zu gewährleisten. Mit unserem IT-Risikomanagement schützen Sie Ihr Unternehmen selbst bei einem Totalausfall vor schlimmen Folgen wie Umsatzeinbußen, Vertrauensverlust bei Ihren Kunden und möglichen Schadenersatzforderungen. Wir sind Ihr Partner. Heute und in Zukunft.

AKTUELL

IT-Compliance EuroSOX 5-Punkte-Plan für Ihre IT.

Die am 1. Juli letzten Jahres in Kraft getretene 8. EU-Richtlinie (EuroSOX) stellt hohe Anforderungen an das Risikomanagement im Unternehmen. Auch ein Jahr nachdem in Deutschland das Gesetz in Kraft getreten ist, besteht in Unternehmen akuter Handlungsbedarf in Bezug auf IT-Sicherheit, um den gesetzlichen Anforderungen gerecht zu werden. Denn nur wenige Unternehmen wissen konkret, was dies für sie bedeutet. Drimalski & Partner hat die wichtigsten Anforderungen von EuroSOX an die IT im Überblick für Sie zusammengestellt.

Lesen Sie mehr unter:
www.drimalski-news.de

Das größte Risiko ist, wenn Sie Ihre Risiken nicht kennen.

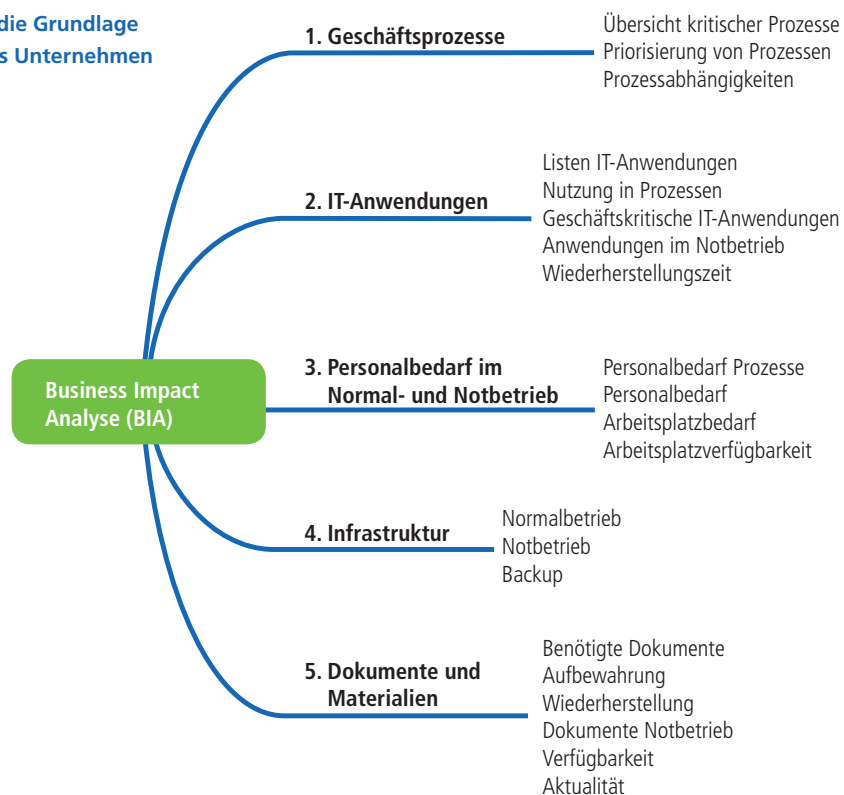
Alles für möglich halten. Nie mehr überrascht werden.

Die Erfahrungen bei schweren IT-Zwischenfällen belegen: Die eigentliche Katastrophe ist die Unwissenheit über mögliche Risiken. Im Ernstfall fehlen eingespielte Prozesse, um auf kritische Situationen geeignet reagieren zu können. Dabei ist eine Notfallplanung unbedingt notwendig: Einbruch, Diebstahl oder ein Zusammenbruch der Stromversorgung, Störungen bei der Online-Anbindung von Datenbanken an die Zentrale oder gezielte Online-Angriffe von außen können unternehmenskritische Systeme langfristig lahm legen oder sogar zerstören. Wer das von vornherein einplant, ist im Fall der Fälle schneller wieder auf der sicheren Seite. Ein gutes IT-Risikomanagement macht das Restrisiko dank integrativer Sicherheitskonzepte kalkulierbar.

Die Lösung ist da, bevor die Probleme auftauchen.

Wir entwickeln für Sie einen maßgeschneiderten, vollständig dokumentierten IT-Notfallplan. Er erlaubt es Ihnen, möglichst rasch wieder zum Tagesgeschäft zurückzukehren, denn er legt die Organisation und das genaue Vorgehen bei Notfällen fest. Das ermöglicht Ihnen die planvolle Wiederherstellung Ihrer Unternehmensprozesse. Erreichen Sie so die größtmögliche Sicherheit für Ihre Geschäftsprozesse und Ihr Unternehmen.

Die Business Impact Analyse bildet die Grundlage für eine Sicherheitsstrategie, die das Unternehmen in Notfällen und Krisen unterstützt.



Maßnahmen unseres IT-Risikomanagements für Ihren IT-Notfallplan:

- **Business Impact Analyse (BIA)**
Sie dient der Darstellung aller geschäftskritischen Unternehmensprozesse und IT-Anwendungen: Sie stellt Abhängigkeiten dar, gibt Antworten auf die Frage, wo von Prozesse und Ressourcen bedroht werden und zeigt somit Schwachstellen in der IT auf.
- **Kritikalitätsanalyse**
Hier werden die kritischen Unternehmensprozesse aus der Gesamtheit der Geschäftsprozesse herausgefiltert.
- **Serverübersicht**
Sie erhalten eine Übersicht über eingesetzte Server und die auf ihnen installierten Applikationen. Es wird eine Einschätzung vorgenommen, wie lange diese im Höchstfall ausfallen dürfen.
- **Schutzbedarfsanalyse**
Die Schutzbedarfsanalyse dient dazu, die Vertraulichkeit, Verfügbarkeit und Integrität von IT-Anwendungen, Daten und Netzwerkkomponenten einzustufen, insbesondere im Hinblick auf die Wirtschaftlichkeit und Existenz eines Unternehmens.
- **Risikostrategie-Optionen**
Hier ergibt sich die Möglichkeit ein Risiko zu akzeptieren, zu vermeiden, zu reduzieren oder an einen externen Dienstleister zu transferieren. Die Ermittlung dient der Entwicklung von Szenarien.
- **Kontinuitätsstrategien**
Festlegung von Strategien, um die Unternehmensprozesse so schnell wie möglich wieder herzustellen und mit welchem Aufwand. Hieraus lassen sich dann Lösungen entwickeln, um die technische Sicherheit zu erhöhen.
- **Notfallvorsorgekonzept**
Das Konzept wird präventiv erstellt und kommt im Notfall zum Tragen. Es beinhaltet risikoreduzierende Maßnahmen.

Alles zusammen ergibt den Geschäftsfortführungsplan.