

Technisches Risk Management

Schulstraße 43a
D-65795 Hattersheim
Telefon: 0 61 90/88 88-0
Telefax: 0 61 90/88 88-30
E-Mail: info@amendi.de

Geänderte IT-Gefährdungslage

Die zunehmende Durchdringung unserer Gesellschaft mit Informations- und Kommunikationstechnik (IuK) und der damit verbundene Wandel zur Dienstleistungs- und Informationsgesellschaft hat für die Unternehmen neue Gefährdungssituationen hervor gebracht. Eine aktive Auseinandersetzung mit dieser geänderten Gefährdungslage ist für jedes Unternehmen unabdingbar geworden, wenn es seine Wettbewerbsfähigkeit erhalten will.

Das unterschätzte Risiko

Kennen Sie die aktuelle Gefährdungslage Ihres Unternehmens?

Diese Frage ist in den meisten Fällen nicht sofort mit einem klaren „Ja“ oder „Nein“ zu beantworten. Erst die aktive Auseinandersetzung mit der möglichen Gefährdungslage bringt die Risiken an den Tag, welche den Unternehmenserfolg gefährden.

Gerne zitieren wir an dieser Stelle das *Bundesamt für Sicherheit in der Informationstechnik (BSI)*, das in seinem „**Leitfaden für IT-Sicherheit (IT-Grundschutz kompakt)**“ mit der weit verbreiteten Ansicht aufräumt, dass IT-Sicherheitsmaßnahmen zwangsläufig mit hohen Investitionskosten verbunden seien. Die wichtigsten Erfolgsfaktoren sind laut BSI gesunder Menschenverstand, durchdachte organisatorische Regelungen und zuverlässige, gut informierte Mitarbeiter, die selbständig Sicherheitsanforderungen diszipliniert und routiniert beachten.

Die Erstellung und Umsetzung eines wirksamen und effektiven IT-Sicherheitskonzeptes muss darum nicht zwangsläufig unbezahlbar sein. Die wirksamsten Maßnahmen sind überraschend simpel und dazu oft noch kostenlos.

Eine weit verbreitete Fehleinschätzung betrifft den eigenen Schutzbedarf.

Vielfach stößt man auf folgende Aussagen:

- **Bei uns ist noch nie was passiert.**

Diese Aussage ist mutig. Vielleicht hat bei früheren Sicherheitsvorfällen niemand etwas bemerkt!

- **Was soll bei uns schon zu holen sein, so geheim sind unsere Daten nicht?**

Diese Einschätzung ist in den meisten Fällen zu oberflächlich. Bei sorgfältiger Betrachtung von möglichen Schadensszenarien zeigt sich schnell: Es können durchaus Daten verarbeitet werden, die vielfältigen Missbrauch ermöglichen, wenn sie in die falschen Hände geraten.

- **Unser Netz ist sicher.**

Die Fähigkeiten potentieller Angreifer werden oft unterschätzt. Hinzu kommt, dass selbst ein erfahrener Netz- oder Sicherheitsspezialist nicht alles wissen und gelegentlich Fehler machen kann. Externe Überprüfungen decken nahezu immer ernste Schwachstellen auf und sind ein guter Schutz vor „Betriebsblindheit“.

- **Unsere Mitarbeiter sind vertrauenswürdig.**

Verschiedene Statistiken zeigen ein anderes Bild. Die Mehrzahl der Sicherheitsverstöße wird durch Innentäter verursacht. Auch durch Versehen, Übereifer oder Neugierde gepaart mit mangelndem Problembewusstsein entstehen manchmal große Schäden.

Was ist zu tun, um den eigentlichen Risiken auf die Spur zu kommen?

Es gilt mit einem möglichst übergreifenden Ansatz ein professionelles Risk Management zu betreiben, in dem Sicherheit als Ganzes betrachtet wird.

Mit unseren Risk Management Services unterstützen wir Sie dabei die Gefährdungspotenziale für Ihre im Einsatz oder in der Planung befindlichen Technologien zu erkennen und durch geeignete Maßnahmen abzubauen.

Sprechen Sie uns doch einfach an. Unsere Spezialisten stehen Ihnen gerne für ein unverbindliches Beratungsgespräch zur Verfügung.

Ihre Amendi GmbH

Ablauf Risk-Management-Prozess:

1. **Gespräch und Bestandsaufnahme**
2. **Risikodefinition**
Ist-Zustand mit den anerkannten Regeln der Technik und geltenden Verordnungen abgleichen
3. **Risikoanalyse**
Analyse der Schwachstellen
4. **Risikosteuerung**
 - Gemeinsame Definierung der Schutzziele
 - Gemeinsame Festlegung der Maßnahmen
 - Unterstützung bei der Umsetzung
5. **Risikoüberwachung**
Permanentes Controlling

Sie finden uns auch im Web:
www.amendi.de