Dr. Wolfgang Straub
Deutsch Wyss & Partner
C.P. 5860
CH-3001 Berne

wolfgang.straub@advobern.ch

Recommandations aux organes de sociétés en matière de sécurité informatique

Mesures sur le plan juridique

– **Définir les responsabilités** pour les systèmes informatiques de l'entreprise

– Assurer une délégation formellement correcte de tâches aliénables

  - Règlement d'organisation
  - Assumer les obligations de diligence lors du choix, de l'instruction et de la supervision de délégués
  - Révision périodique de l'étendue de la délégation

– Communiquer des **conflits d'intérêts** et respecter les règles d'incapacité

– Effectuer un **contrôle de plausibilité** des requêtes proposées par les délégués, des experts ou des autres membres du conseil d'administration/de la direction

Mesures sur le plan organisationnel

– Développer un **concept** pour l'utilisation des moyens informatiques dans l'entreprise

– Observer les standards et ***best practices*** courants dans la branche et obliger les partenaires contractuels à les respecter

– Déclencher un **processus de sécurité d'informatique**

  - Définir des objectifs et une stratégie de sécurité
  - Effectuer une analyse de sécurité

  - Développer un concept de sécurité/des directives de sécurité
  - Mettre à disposition les moyens nécessaires et développer une culture de sécurité
  - Intégrer les partenaires contractuels dans le processus

– **Certifier** des procédures et systèmes

– Assurer l'**information et des contrôles** appropriés (effectuer des *IT security audits* et inscrire régulièrement la question de la sécurité informatique à l'ordre du jour du conseil d'administration)

– Instaurer un *risk management* adéquat pour les **contrats** informatiques (analyse et optimisation continue des risques lors de la négociation et de la mise en œuvre des contrats)
  - Minimiser les risques sur le plan juridique et organisationnel (p.ex. solvabilité/garanties d'accomplissement)
  - Prendre conscience des risques résiduels
  - Prévoir des réserves adéquates pour les risques résiduels

– **Documenter** la mise en œuvre de la diligence à tous les niveaux (p.ex. prises de décisions, mesures de sécurité)

– Conclure une **assurance D&O** avec couverture adéquate

Références de littérature

Voir les recommandations pratiques dans les ouvrages suivants:

BAUEN MARC/VENTURI SILVIO, Le conseil d'administration: organisation, attributions, responsabilité, corporate governance, Zurich 2007, n. 777ss.

FORSTMOSER PETER/SPRECHER THOMAS/TÖNDURY GIAN ANDRI, Persönliche Haftung nach Schweizer Aktienrecht, Zurich/Bâle/Genève 2005, p. 109ss.

JÖRG FLORIAN S., Das Mitglied des Verwaltungsrats als Superman? Pflichten und Tipps, in Jörg Florian S./Arter Oliver (éds): Entwicklungen im Gesellschaftsrecht I, Berne 2006, p. 279ss.

MÜLLER ROLAND, unsorgfältige Führung eines Verwaltungsratsmandats, in Geiser Thomas/Münch Peter (éds), Schaden – Haftung – Versicherung, Bâle/Genève/Munich 1999, p. 861ss.

MÜLLER ROLAND/LIPP LORENZ/PLÜSS ADRIAN, Der Verwaltungsrat – ein Handbuch für die Praxis, 3. éd. Zurich 2007, p. 365ss.

SCHNEIDER JÜRG, Informationssicherheit in der IT und persönliche Haftung der Verwaltungsräte, Bâle/Genève 2008, p. 48ss.

WEBER ROLF H., Elektronische Aufbewahrung und Archivierung, recht 2004, p. 76s.

Standards & Best Practices (énumération non exhaustive)

BUNDESAMT FÜR SICHERHEIT IN DER INFORMATIONSTECHNIK (BSI): IT Grundschutz-Kataloge, disponibles sur le site: *www.bsi.bund/de*

CONSEIL DE L'INFORMATIQUE DE LA CONFEDERATION (CI), Directives concernant la sécurité informatique dans l'administration fédérale, disponibles sur le site *http://www.isb.admin.ch/themen/sicherheit*

ECONOMIESUISSE, Swiss Code of Best Practice for Corporate Governance (SCBP), disponible sur le site *www.economiesuisse.ch*

INORMATION SECURITY FORUM (ISF): Standard of Good Practice for Information Security, disponible sur le site www.securityforum.org/index.htm

INFORMATION SYSTEMS AUDIT AND CONTROL ASSOCIATION (ISACA), Control Objectives for Information and Related Technology (COBIT) *www.isaca.org/cobit.htm*

INTERNATIONAL STANDARD ORGANIZATION (ISO): normes ISO/IEC 17799 : 2005 ; ISO/IEC 27001:2005; ISO/IEC 27002:2005; ISO/IEC 27006:2007; ISO/IEC 13335:2004; ISO/IEC 15408:2005; ISO/IEC 15408-3:2005; ISO/IEC 23081:2006; ISO/IEC 20000:2005 disponibles sur le site *www.iso.org*

OFFICE OF GOVERNMENT COMMERCE (OGC), Information Technology Infrastructure Library *http://www.ogc.gov.uk/guidance_itil.asp*