Deutsch Wyss
& Partner

Forum Suisse pour le Droit de la Communication
Université de Genève

Séminaire du 28 novembre 2008

Devoirs et responsabilités des organes de sociétés en matière de sécurité informatique

Wolfgang Straub

Plan de l'exposé

- Les devoirs de l'entreprise en matière informatique
- La responsabilité des organes
- Comment éviter d'engager sa responsabilité

2

Cas pratique

Incendie dans un data center causé par un bloc d'alimentation électrique

→ dommage hardware → perte de données → perte de production → prétentions de clients

- Prétentions contractuelles contre le **fournisseur** →limitation par des obligations de prévention et de diminution du dommage (*Business Continuity Management*)
- Prétentions contractuelles contre les **collaborateurs** responsables (art. 321e CO)
- Responsabilité des **organes**?

3

Les devoirs de l'entreprise

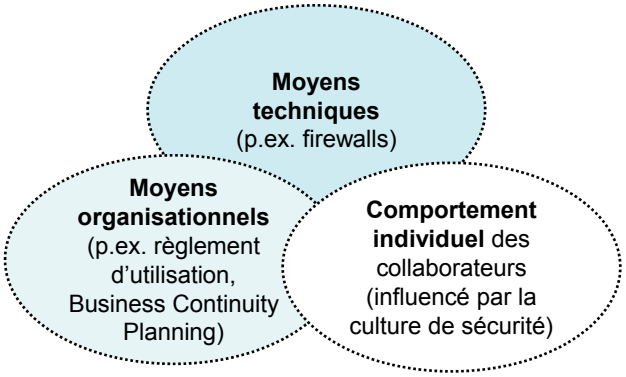
Les objectifs de la sécurité informatique

- **Disponibilité** et efficacité des systèmes et des données
- **Confidentialité** des données (protection contre prise de connaissance par des personnes non habilitées)
- **Intégrité** des données (protection contre destruction et manipulation)
- **Caractère démontrable** de la confidentialité et de l'intégrité des données

4

Les devoirs de l'entreprise

Les éléments de la sécurité informatique



5

Les devoirs de l'entreprise

Les devoirs de confidentialité de l'entreprise

- → **Protection de données** (LPD)
- → **Archivage de documents** commerciaux électroniques (Olico)
- → **Secrets professionnels**, p.ex. dans le domaine médical/judiciaire (cf. aussi les art. 321 et 11 CP)
- → **Obligations sectorielles** (p.ex. télécommunications)
- → **Obligations contractuelles** envers des clients et des fournisseurs

6

Les devoirs de l'entreprise

Les devoirs d'information de l'entreprise

- → Devoirs de preuve et d'archivage en **matière fiscale** (voir p.ex. les art. 125s. LIFD et 57s. LTVA)
- → Conservation des livres de compte (**Olico**)
- → **Comptabilité** basée sur une analyse de risques concevable
- → Obligations **sectorielles** (p.ex. analyse des risques opérationnels dans le cadre de Bâle II)
- → Obligations **contractuelles**

7

Cas pratique

Attaque 'SQL injection' contre un webshop
→ Les données personnelles des clients des 15 derniers années ont été partiellement manipulées

- Est-ce que les mesures de sauvegarde courantes ont été mises en œuvre?
- Pourquoi est-ce que des données périmées ont été sauvegardées?
- Violation de la LPD
- Atteintes à l'image de l'entreprise
- Dommages-intérêts?

8

Les devoirs de l’entreprise

Causes récurrentes de dommages

- **Défauts** de conception/mise en œuvre de systèmes IT
- **Mauvaise utilisation** des systèmes informatiques
- Influence de l’infrastructure de base
- Prestations déficientes de **fournisseurs** (p.ex. outsourcing provider)
- **Attaques** par des collaborateurs ou des tiers
- Manque de diligence lors de l’évaluation de **risques**
- Manque de mesures de **sauvegarde**, *Business Continuity Management*

9

La responsabilité des organes

Qui tombe sous le coup des art. 754ss CO?

Les fondateurs

Le conseil d‘administration

La direction de l‘entreprise

- Le premier niveau de direction (CEO, CIO etc.)
- Des collaborateurs subordonnés seulement dans des circonstances exceptionnelles
- Des organes factuels

Les réviseurs

10

Cas pratique

Une société de production chimique est rachetée.
Un accident grave est causé par le système informatique vétuste.
Les risques de production n'ont pas été pris en compte ni dans le prix de rachat ni dans les bilans.

→Responsabilité des organes?

11

La responsabilité des organes

La responsabilité des organes en matière informatique

- Dommages causés par **négligence** en matière de sécurité informatique
- **Pertes** qui auraient été **évitables** par des mesures des sauvegarde (p.ex. *Disaster Recovery Planning*)
- Erreurs lors de l'établissement du bilan causées par une **évaluation incorrecte** des risques liés à l'informatique

12

La responsabilité des organes

Les conditions de la responsabilité

- Manque de diligence lors d'une **activité** ou **inactivité malgré un devoir** d'action
- **Légitimation active**: la société, les actionnaires et – en cas de faillite – les créanciers
- **Fardeau de la preuve**: demandeur, mais perception objective de la diligence
- **Décharge**: délai de 6 mois pour les actionnaires qui n'ont pas donné décharge au conseil d'administration
- **Prescription**: délai de 5 ans depuis la connaissance et de 10 ans depuis la naissance du dommage

13

La responsabilité des organes

La responsabilité du conseil d'administration

Les attributions inaliénables (haute direction et haute surveillance):

- Désignation des **objectifs stratégiques** en matière informatique
- Instauration d'un **processus d'analyse et d'optimisation** en matière de sécurité informatique
- **Définition des responsabilités** en matière informatique
- **Surveillance** (rapports périodiques des responsables)
- Système de **contrôle interne** et **risk management** (art. 728a CO et art. 19 SCBP)

14

La responsabilité des organes

La délégation de devoirs…

- doit être dans **l'intérêt de la société**
- doit être **admise** par le CO et les statuts (év. concrétisés par le règlement d'organisation)
- doit reposer sur une **décision formelle** du conseil d'administration

→**responsabilité limitée** (diligence lors de l'organisation du travail, du choix, de l'instruction et de la surveillance des délégués internes ou externes)

Si les **conditions ne sont pas remplies**, le déléguant répond du dommage comme s'il l'avait causé lui-même

15

La responsabilité des organes

La responsabilité de la direction

- Création et mise en œuvre d'un **concept de sécurité informatique** et réexamen périodique
- **Organisation et surveillance** adéquate des processus reliés à l'informatique
- **Compliance** avec les standards requis par le droit et les best practices (art. 20 SCBP)
- **Subdélégation** correcte
- Mise à disposition des **ressources** nécessaires
- Encouragement d'une **culture** de la sécurité informatique

16

La responsabilité des organes

Le niveau de diligence requis…

...dépend de l'importance de l'informatique pour l'entreprise

- **Perception objective** de la diligence, mais l'expertise de certains membres sera prise en compte
- Les **membres qui ne participent pas** au processus de la prise de décisions restent responsables
- Importance du degré de la faute lors de la répartition du dommage entre **plusieurs responsables**

17

La responsabilité des organes

Le niveau de diligence requis

- Importance des **standards** et ***best practices*** (p.ex. ISO/IEC 17799, COBIT, Grundschutzhandbuch, ITIL, Directives du conseil informatique de la Confédération concernant la sécurité informatique dans l'administration fédérale, Circulaire CFB 99/2 «Outsourcing»)
- Importance de **certifications** (p.ex. ISO)?
- **Documentation** de la diligence

18

La responsabilité des organes

Protection de la liberté d'appréciation et de décision des stakeholders par la ***Business Judgment Rule***?

Limites:

- Décisions formellement incorrectes
- Conflits d'intérêts non déclarés
- Décisions incorrectes d'un point de vue ex ante

19

Cas pratique

Archive de plans de construction détruit par submersion

→ Coûts de rétablissement de CHF 120 mio. (il n'y avait pas de copies de sauvegarde)

→ Les assurances invoquent des obligations de prévention

→ Responsabilité des organes pour négligence?

20

Comment éviter la responsabilité

US Federal Trade Commission

Obligation de mettre en œuvre un programme complet de sécurité d'information, contenant notamment

- la répartition des **responsabilités** (désignation de personnes responsables)
- une **analyse des risques**
- l'implémentation de **mesures de sauvegarde**
- la **maintenance** des éléments de sécurité
- des **réexamens** périodiques (audits)

21

Comment éviter la responsabilité

Analyse de risques

- Quelle est la **probabilité** du risque?
- Quel serait **l'impact** (dégâts possibles)?
- Quelles sont les **coûts** des mesures de sauvegarde?
- Quel serait l'impact des mesures de sauvegarde (**taux de réussite** vs. **effets négatifs** sur d'autres domaines)

22

Comment éviter la responsabilité

Analyse des risques (exemple)

Ten-dance	Description du risque	Proba-bility	Impact	Risk factor	Mesures à prendre
⇨	Incendie	3	4	12	Scanning de tous les documents imprimés, backup data center
⇧	Vol hardware	3	3	9	Terminal server, login avec support biométrique
⇨	Panne de courant	3	3	9	Génératrice de secours
⇩	Accès internet bloqué	3	3	9	Connexions à plusieurs fournisseurs d'accès
...	...	...	...	...	...

Probabilité: Probabilité de la réalisation du risque (1: faible, 2: plutôt faible, 3: moyen, 4: plutôt haute, 5: haute)
Impact: Effets en cas d'une réalisation du risque (1: faible, 2: plutôt faible, 3: moyen, 4: plutôt haut, 5: haut)
Risik Factor: Multiplication de probability x impact

23

Comment éviter la responsabilité

Mesures sur la plan juridique

Définir les responsabilités pour les systèmes informatiques de l'entreprise

- **Règlement d'organisation**
- **Délégations** formellement correctes
- **Contrôle de plausibilité** des propositions des experts
- Assumer les **obligations de diligence** lors du choix, de l'instruction et de la supervision des délégués
- **Réexamen** périodique de l'étendue **de délégations**

24

Comment éviter la responsabilité

Mesures sur le plan juridique

Communiquer des **conflits d'intérêts**

Inscrire régulièrement la situation de sécurité informatique à **l'ordre du jour du conseil** d'administration

Conclure une **assurance D&O** avec couverture suffisante

25

Comment éviter la responsabilité

Mesures sur le plan juridique

Instaurer un ***risk management* 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 et accepter les risques résiduels
- Prévoir des réserves adéquates pour les risques résiduels

26

Comment éviter la responsabilité

Mesures sur le plan organisationnel

- Développer un **concept** pour l'utilisation des moyens informatiques dans l'entreprise (*IT Strategy*)
- Observer les standards et ***best practices*** courants dans la branche et les imposer aux partenaires contractuels
- **Documenter** la propre diligence (p.ex. prises de décisions, mesures de sécurité)
- **Certifier** des procédures et des systèmes
- Effectuer des ***IT Security Audits***

27

Comment éviter la responsabilité

Mesures sur le plan organisationnel

Déclencher un **processus de sécurité 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
- Intégrer les partenaires contractuels

28

Conclusions

- Pas tous les risques peuvent être évités (conflits entre des objectifs différents, coûts). → Certains risques doivent être acceptés.
- Ceux qui analysent les risques ne devraient pas être pénalisés par rapport à ceux qui ne s'en occupent pas
- Le responsabilité pour la sécurité informatique ne peut pas être entièrement déléguée (même dans l'hypothèse d'un full outsourcing des systèmes informatique).

29

Questions, critiques, remarques etc.?

Wolfgang Straub
Deutsch Wyss & Partner
Effingerstrasse 17/C.P. 5860
CH-3001 Berne

+41 31 381 44 25

wolfgang.straub@advobern.ch
www.advobern.ch

30