



# LA SECURITE : ORGANISATION ET TECHNOLOGIES





## Copyright

Tous droits réservés IDactis. Ce white paper ne peut être reproduit, en partie ou en totalité, sans la permission écrite préalable d'IDactis.

© 2004 IDactis

## Marques déposées

Toutes les marques citées dans ce manuel sont la propriété de leurs détenteurs respectifs. IDactis™, IDactis Security™, ID>Lock™ et ID>Pass™ sont des marques déposées.

N'hésitez pas à nous contacter à [support@idactis.com](mailto:support@idactis.com) pour toute information technique ou [sales@idactis.com](mailto:sales@idactis.com) pour toute information commerciale.



## TABLES DES MATIERES

1.	La technologie seule n'est pas un remède .....	4
2.	Organiser la sécurité .....	4
2.1.	Identifier et analyser les risques .....	4
2.2.	Définir des objectifs de sécurité .....	5
2.3.	Appliquer la politique de sécurité .....	5
2.4.	Contrôler la sécurité .....	6
3.	En résumé .....	6

# 1. La technologie seule n'est pas un remède

« Science sans conscience n'est que ruine de l'âme » : cette célèbre phrase de Rabelais permet d'illustrer une tendance relativement préoccupante en terme de sécurité informatique : la prépondérance de la technologie sur l'organisation.

Autrement dit, on observe que beaucoup de sociétés :

- réagissent à posteriori en cas d'incidents liés à la sécurité informatique,
- acquièrent et utilisent une technologie comme un remède, en pensant que cela ira mieux.

Toutefois, certains remèdes ne traitent que les symptômes et non la cause, et, comme chacun le sait, il vaut souvent mieux prévenir que guérir. En d'autres termes, la sécurité informatique ne se limite pas à l'utilisation de technologies éprouvées ou émergentes, mais repose, avant tout, sur une stratégie d'ensemble et sur des processus organisationnels.

En effet, la mise en place de solutions permet de se donner bonne conscience et de traiter ponctuellement des failles sécuritaires. Toutefois, l'impact organisationnel et financier de la mise en place, insuffisamment évaluée, d'une solution peut s'avérer désastreux. Exemples :

- Un pare-feu trop restrictif qui interdit des sites de consultation de BDD financières utiles à des conseillers financiers (approche métier insuffisamment appréhendée),
- Des utilisateurs incapables d'accéder à leur PC suite à un oubli ou perte de token (procédure d'urgence insuffisamment évaluée),
- Des informations vitales cryptées, perdues suite au départ d'un salarié (pas de mise en place d'une clé de recouvrement ou de sauvegarde d'une clé utilisateur),
- etc.

Le risque est avant tout dû au facteur humain : c'est d'abord de ce côté qu'il faut chercher.

## 2. Organiser la sécurité

Il est donc primordial d'adopter une approche stratégique du risque (risques internes et externes) et de décliner cette stratégie en termes techniques et organisationnels.

### 2.1. *Identifier et analyser les risques*

Identifier et analyser les risques revient à évaluer les risques internes et externes, afin de déterminer les menaces et faiblesses en terme de sécurité. Il convient également d'appréhender les opportunités et les forces qui existent au sein et à l'extérieur de l'entreprise.

Les risques externes et internes peuvent être identifiés et évalués en s'intéressant aux différents acteurs de l'entreprise : employés, clients, fournisseurs, organismes sociaux, etc. et particulièrement en évaluant le plus complètement possible l'ensemble des flux d'information : qui échange avec qui et quoi. En fonction de cette cartographie, on peut classer les flux d'informations (y compris non numériques) en catégories à risque ou non, et susceptibles d'être sécurisées ou non.

Il est nécessaire également d'évaluer le niveau de sensibilisation des acteurs à la sécurité, de mesurer les coûts induits par des failles sécuritaires (ex. vols de brevets, de fichiers clients, mais aussi non respect de réglementations juridiques etc.).

L'ensemble de ces évaluations doit permettre d'obtenir une liste exhaustive des faiblesses et menaces internes et externes auxquelles doit faire face l'entreprise. Ces mesures qualitatives et quantitatives

doivent permettre également d'identifier les forces et les opportunités qui viendront renforcer la politique de sécurité à mettre en œuvre.

Secteurs de risques (liste non exhaustive)	Salariés	Fournisseurs	Clients
Risque informatique : <ul style="list-style-type: none"> <li>• Applications métiers</li> <li>• Applications communes (messagerie, Internet, etc.)</li> <li>• Applications particulières (logiciel peer to peer, etc.)</li> <li>• Accès aux PC</li> <li>• Nomades</li> <li>• Sauvegardes</li> <li>• Plan de continuité</li> <li>• Etc.</li> </ul>			
Risque non informatique : <ul style="list-style-type: none"> <li>• Accès locaux</li> <li>• Téléphone (social engineering)</li> <li>• Réglementations juridiques et sociales</li> <li>• Sensibilisation des acteurs</li> <li>• Image</li> <li>• Savoir faire</li> <li>• Etc.</li> </ul>			

## 2.2. Définir des objectifs de sécurité

En fonction des risques et des atouts précédemment identifiés, on définit ensuite des objectifs de sécurité. Ces objectifs doivent être mesurables, spécifiques, atteignables, réalistes et planifiés.

A ce stade, on définit également un plan d'action, ainsi que le ROI et budgets prévisionnels. Des arbitrages interviennent fréquemment en fonction des priorités budgétaires : la sécurité est un processus qui s'inscrit dans le temps, aussi il ne faut pas hésiter à définir un plan sur plusieurs années.

## 2.3. Appliquer la politique de sécurité

C'est à ce stade que la technologie doit intervenir : lorsque l'impact financier et organisationnel de la sécurité a été évaluée et planifiée. Cette technologie doit traduire les objectifs définis précédemment.

Inutile de préciser que l'adhésion de tous les acteurs, et avant tout celui du management, en particulier la DG, est un facteur incontournable pour le succès lié à la mise en place de technologies sécuritaires, souvent contraignantes.

Exemple : un objectif de sécurité est : « sécuriser les PC nomades des managers », parce que l'on a identifié un risque de compromission d'information en cas de vol du portable. Appliquer la politique de sécurité reviendra à :

- Identifier les managers avec portable et les applications/méthodes de travail,
- Choisir une solution de chiffrement,
- Déployer la solution en mettant en œuvre les différents mécanismes (création de clés de groupes, clés personnelles, clé de recouvrement, disques chiffrés, etc.)
- Former et sensibiliser les managers
- Mettre en place une procédure de help desk

Les exemples sont fréquents où une décision est prise de sécuriser des portables, sans avoir préalablement déterminé la manière dont travaillent les utilisateurs, leur manière de sauvegarder, les informations à protéger, la procédure en cas de pertes de clés, qui émet les clés, etc. Les conséquences peuvent être désastreuses (solution non ou mal utilisée, perte de données, blocages d'utilisateurs, etc.).

## **2.4.     *Contrôler la sécurité***

Contrôler la sécurité revient à définir et mettre en place des tableaux de bord synthétiques et détaillés en fonction du type de population visée : synthétique pour la DG et détaillée pour le RSSI.

Ces tableaux serviront à valider et corriger les objectifs de sécurité définis.

## **3. En résumé**

On pourrait résumer ce texte par le vieil adage populaire « il ne faut pas mettre la charrue avant les bœufs » : la technologie ne représente que 20% de la réussite d'une stratégie sécuritaire en entreprise. En effet, le facteur humain est primordial : vous n'empêchez jamais un utilisateur de divulguer son code utilisateur et mot de passe, mais vous le dissuaderez fortement si vous le sensibilisez aux conséquences pour l'entreprise et surtout pour lui-même en cas de malveillance lié à son login.

Avant d'acquérir et de déployer une technologie de sécurité, il convient d'identifier ses vulnérabilités en appréhendant l'ensemble des flux d'information entre les différents acteurs de l'entreprise.

Ensuite, des objectifs de sécurité sont définis : ils s'inscrivent dans un plan stratégique et budgétaire sur plusieurs années.

Enfin, la technologie entre en jeu et vient concrétiser les objectifs de sécurité qui seront contrôlés régulièrement afin de piloter la politique de sécurité.