

De la Théorie de la Confiance à la Pratique du Contrôle

Par Denis Lechevin, Advens

La confiance, moteur de la Sécurité de l'Information ne s'acquiert que par le biais de contrôles a priori ou a posteriori. Or si les entreprises mettent en œuvre facilement des contrôles a priori (blocage de flux par un firewall par exemple), elles s'engagent difficilement dans les contrôles a posteriori. Avec le développement des technologies de grande consommation, cette approche peut s'avérer trop étroite pour offrir toute la confiance nécessaire au développement des entreprises. Chez Advens, nous croyons qu'une nouvelle voie est possible, complémentaire mais totalement novatrice : « l'autonomie contrôlée des utilisateurs ».

La confiance est à la base de toute relation d'échange et/ou d'interaction qui peut comporter des risques. Et la notion de confiance prend toute son importance dès lors qu'elle participe à la création de valeurs et de prospérité comme l'évoque Fukuyama dans son best seller « *Trust: the social virtues and the creation of prosperity* » (1995). Les avis divergent sur les liens de causalité entre la confiance et la création de valeur¹ mais s'accordent sur la nécessité de mécanismes de contrôle a priori (ex ante) et a posteriori (ex post) divers et variés parmi lesquels les contraintes sociales, les mécanismes de réputation, etc. Notons que les mécanismes de contrôle axés sur des démarches qu'a priori ou qu'a posteriori sont en plus écartés car trop étroits pour être totalement efficaces (« *Le rôle de la confiance dans le système de gouvernance des entreprises* », Charreaux 1998).

Lorsque les solutions de « contrôle a priori » - traditionnelles - ont atteint leurs limites, l'entreprise doit s'engager dans une démarche de contrôle a posteriori.

Les concepts de sécurité de l'information trouvent eux aussi une légitimité autour de la confiance: la confiance dans le système d'information, la confiance dans les informations, la confiance dans la relation entre deux individus. La sécurité de l'information crée un espace de confiance qui, dans le contexte des entreprises, permet le développement de valeur et de prospérité. L'usage des technologies de l'information au service de la performance de l'entreprise n'est autorisé qu'au prix de l'acceptation des risques inhérents à cet usage. Ex : la création d'un site WEB, l'ouverture du système d'information à l'Internet en

vue d'un échange avec de nouveaux partenaires entraîne en retour la possibilité d'actes de malveillance en provenance de l'Internet. L'entreprise n'accepte ce risque que dans la mesure où elle peut mettre en œuvre des contrôles a priori comme un firewall.

Là où la pratique fait défaut c'est que l'entreprise s'applique trop souvent à vouloir contrôler a priori (bloquer) ce qu'elle ne maîtrise pas et qui réduit l'espace de confiance nécessaire à son développement. Ce phénomène principalement lié au concept du « *Plug & Forget* » s'explique principalement parce que les contrôles a priori sont faciles à adresser par des solutions « *qu'on installe et qu'on oublie* » alors que les contrôles a posteriori nécessitent des procédures. L'entreprise se place alors dans la situation restrictive de ne proposer que des contrôles a priori, au prix de la mise en œuvre de solutions (trop) complexes, (trop) coûteuses, inadaptées à son contexte car limitant les actions de ses utilisateurs.

Et cela est d'autant plus vrai que l'émergence des technologies de grande consommation (qui apportent des bénéfices certains dans la performance de l'entreprise) a radicalement changé les menaces de Sécurité auxquelles sont exposées les entreprises. Chris Young, Vice Président de RSA Security, évoquait justement cet aspect lors de la RSA Conference Europe 2009 de Londres: « *Les services informatiques ont tenté de résister à l'arrivée des BlackBerry ou d'interdire l'utilisation de l'iPhone - certains d'entre nous ont même essayé de combler les ports USB à l'époxy pour empêcher la copie de fichiers sur des clés USB alors que cette résistance est futile et contre-productive dans de nombreux cas.* »

Chris Young révèle aussi la nécessité d'un changement de mentalité nécessaire dans la pratique du contrôle : « *Essayer d'empêcher l'utilisation des nouvelles technologies attrayantes dans les entreprises, surtout si on les retrouve dans les foyers familiaux, est le meilleur moyen pour nous, professionnels de la sécurité, de devenir inutile. Les organisations qui rejettent ces tendances seront probablement mises hors compétition.* » C'est un message partagé par Advens et nous pensons qu'il est nécessaire de mettre en œuvre une nouvelle approche du contrôle en lien avec les évolutions de la société.

Parce que la société évolue progressivement d'un modèle établi a priori, prétendant tout réglementer vers le contrôle a posteriori fondé sur « *l'intelligence collective* », Advens a construit cette nouvelle approche du contrôle autour de cette idée que lorsque les solutions de « *contrôle a priori* » - traditionnelles - ont atteint leurs limites, l'entreprise doit s'engager dans une démarche complémentaire de contrôle a posteriori. Ex : dans le cas des clés USB, plutôt que de chercher à en limiter l'usage, éduquons nos utilisateurs et contrôlons a posteriori l'usage qu'il en est fait.

Cette démarche a deux avantages principaux, elle rend « *réellement* » les utilisateurs, acteurs de la sécurité de l'information de leur entreprise et engage un cercle vertueux d'amélioration continue. Advens a toujours souhaité porté le message que le besoin client est toujours légitime et la politique de la muraille n'est pas une réponse, il faut offrir de nouveaux « *horizons* » aux utilisateurs, plus d'autonomie pour plus de compréhension des enjeux de sécurité de l'information.

L'information n'a jamais aussi vite circulée qu'aujourd'hui alors il est temps que l'entreprise s'approprie et concrétise les vieux adages : « *Si tu donnes un poisson à un homme, il mangera un jour. Si tu lui apprends à pêcher, il mangera toujours.* » Il ne dépend que de nous pour offrir aux utilisateurs les moyens de gagner en compétences, en confiance

et donc de participer à l'amélioration du niveau de Sécurité. ■

¹ Fonction de sécurisation des échanges pour Shleifer et Vishny en 1997 ou Lattitude managériale pour Charreaux en 1997

A propos d'Advens

Advens est une société de conseil spécialisée en management de la sécurité de l'information.

Depuis plus de 10 ans, nous aidons les organisations à piloter la sécurité de l'information en parfait alignement avec leurs enjeux métier et pour en améliorer la performance.

Une approche unique qui repose sur une expertise sectorielle pointue dans les domaines de la distribution, de la finance, de l'industrie, de la santé, des services ou de l'administration publique et aide les RSSI à construire une fonction sécurité efficace et valorisée.

Avec des bureaux à Lille et à Paris et une équipe de spécialistes expérimentés, Advens compte parmi ses clients des entreprises leader sur leur marché telles qu'Arcelor Technologies, Auchan, le Groupe Crédit Agricole, Cofidis, Decathlon, Eurotunnel, la Société des Paris Sportifs ou encore le Ministère de l'Education Nationale.

PARIS

5, rue du Helder, 75009 Paris
Tel : +33 (0)1 53 24 00 70
Fax : +33 (0)1 53 24 53 39

LILLE

47, rue du Faubourg de Roubaix
Lille Europe - 59000 Lille
Tel : +33 (0)3 20 68 41 81
Fax : +33 (0)3 20 70 54 28

www.advens.fr
