Chapitre 3 – Les aspects relatifs à la sécurité

par Vincent GAUTRAIS

Introduction

Malgré l'importance croissante que les acteurs lui accordent actuellement, la sécurité des réseaux informatiques demeure la moins organisée et la plus négligée des quatre principales dimensions du commerce électronique (juridique, commercial, technique et sécurité). Responsable d'une école en sécurité informatique, Nicolas SADIRAC prétend à ce titre que les entreprises se contentent de propagande et occultent l'ignorance de la population quant aux problèmes de sécurisation des transactions. Les succès de certains pirates informatiques à interrompre le fonctionnement de sites commerciaux réputés semblent lui donner raison. D'ailleurs, les spécialistes s'accordent sur le fait que la question n'est pas de savoir *qui* va être touché par des intérêts malvaillants (*hacking*) ou négligents mais plutôt *quand*.

Des raisons économiques et sociales expliquent l'attitude passive des commerçants électroniques à l'endroit de la sécurité. D'abord, l'évolution agitée de la nouvelle économie implique des investissements rapides rarement compatibles avec l'implantation onéreuse d'une structure de sécurité. La sécurité est une science « transversale » qui se place au-dessus des structures organisationnelles traditionnelles et nécessite la participation de tous les acteurs d'une compagnie – ainsi que de spécialistes rares et coûteux. Par exemple, un chef de service n'a pas toujours l'habitude de se référer à d'autres intervenants susceptibles, de surcroît, de remettre en cause ses pratiques comportementales. En somme, la sécurité demande des investissements et des ajustements structurels que les entreprises en ligne préfèrent souvent oublier. L'absence de conscientisation collective caractérise également la dimension sécuritaire du commerce électronique.

Alors que la gestion de l'information papier est chose connue, la gestion de l'information électronique balbutie et demeure en réalité une bien faible priorité. Au même titre que la vente à distance exigea au début du vingtième siècle une structure relationnelle solide, une vitrine efficace de commerce électronique requiert un encadrement sécuritaire stable. Le présent chapitre vise à montrer qu'il n'y aura pas, demain davantage qu'aujourd'hui, de commerce électronique sérieux et durable sans la mise en place d'une véritable structure organisationnelle de sécurité.

Néanmoins, nous voudrions éviter de faire des chevauchements avec certains aspects déjà explicités ailleurs en traitant davantage de la sécurité organisationnelle que de la sécurité technique. En ce sens, nous voulons envisager les procédures qui peuvent être mis en place par un responsable de site afin que les transactions électroniques qu'il compte encadrer le soit diligemment. Or, la sécurité informatique est généralement associée à des techniques de chiffrement, à des certificats ou autres techniques de communication. Une

transaction électronique est pourtant tri-temporelle et se situe par conséquent avant, pendant et après l'échange de données. En conséquence, une chaîne d'opération relatant les différentes étapes de la transaction électronique doit être mise en place afin d'identifier chacune des sources de vulnérabilité. À chacun de ces éléments, une solution ou une série d'éléments de protection doit être installée, avec toujours un degré de perfectionnement différent selon chaque situation factuelle, chaque site Internet.

Dans cet ordre d'idée, nous indiquons dans les sections de ce chapitre les démarches à suivre lors d'un processus de mise en place d'une sécurité organisationnelle et étudions les éléments centraux des politiques de sécurité ainsi que les aspects contractuels afférents. En effet, les contrats disposent d'éléments de formalisme qui encadrent les risques d'une relation d'affaire. À cet égard, l'entente contractuelle prendra une forme différente selon le type de la relation et l'ampleur des enjeux en cause. Il est donc fondamental de ne pas oublier l'environnement général qui entoure le contrat.

L'implantation d'une sécurité organisationnelle

Bien que peu de pratiques préexistent en la matière, il est possible d'affirmer que l'organisation sécuritaire s'articule généralement autour de deux sortes de documents : la **politique** de sécurité qui prévoit les principes généraux et les **procédures** qui établissent davantage les détails. Cette démarche à deux niveaux permet une plus grande faculté d'adaptation en cas de modification, de mise à jour. Par exemple, si une entreprise change son système d'exploitation, il est vraisemblable de croire que la politique demeure valide alors que les procédures doivent être ajustées. Ces dernières permettent également de veiller à ce que des difficultés ponctuelles, telles que l'utilisation de procédés instables ou dangereux, soient corrigées.

Le contenu d'une sécurité organisationnelle se compose d'éléments obligatoires pour les intervenants mais aussi, et particulièrement dans le cadre de grosses entreprises, d'indications facultatives qui ont valeur de recommandations. Celles-ci visent essentiellement des fins d'adaptation. Ainsi, on intègre des éléments de sécurité qui devront être appliqués ultérieurement, laissant un délai aux personnes concernées pour s'habituer aux changements.

En principe, une sécurité organisationnelle impose donc des obligations aux différents acteurs de l'entreprise. À cet égard, des sanctions allant de l'avertissement au congédiement doivent être établies par classe, c'est-à-dire en fonction du niveau de gravité de chacun des manquements identifiés. Cette classification a pour but, d'une part, de faire prendre conscience de l'intérêt en cause et, d'autre part, de responsabiliser tout un chacun sur son rôle respectif. Des sanctions de nature pénale peuvent également être soulignées et les poursuites éventuelles peuvent être publicisées. Les personnes concernées, employés, consultants ou autres, devraient pouvoir prendre connaissance de leurs responsabilités et de leurs conséquences tant par le biais de leurs contrats de travail que par des rappels réguliers transmis selon une fréquence déterminée.

Afin d'établir les principes qui guident l'élaboration d'une sécurité organisationnelle, il nous a été nécessaire d'observer ce qui se fait dans un certain nombre d'organisations, d'ailleurs souvent non commerciales. En effet, les entreprises du secteur privé sont peu portées à diffuser leur structure organisationnelle de sécurité, notamment pour des raisons de concurrence mais parfois aussi de sécurité. En revanche, l'encadrement sécuritaire de

l'information électronique a été traité aussi bien par des institutions gouvernementales, des universités, des regroupements sectoriels de commerçants que des autorités de certification. Bien que leurs politiques disposent chacune d'une structure propre, des éléments de rapprochement sont identifiables et peuvent être regroupés autour de six points, à savoir : l'organisation administrative, la structure humaine, l'environnement physique, l'encadrement technique, la communication et les opérations. Ces points font l'objet des sections qui suivent.

L'organisation administrative

Ce premier élément correspond en fait à une réponse à donner aux questions suivantes : qui sont les personnes responsables de la sécurité du site Web envisagé, quels sont les éléments à protéger et quelles sont les procédures permettant d'y parvenir ?

► Les personnes responsables

En premier lieu, il importe de déterminer quelles sont les personnes responsables de la mise en place de la sécurité. Si l'importance de l'entreprise le permet, il est d'abord souhaitable de répartir les responsabilités pour éviter que la sécurité ne repose sur une seule personne. Afin d'obtenir un niveau de sécurité acceptable, les besoins en ressource humaine doivent être évalués et les tâches respectives des personnes concernées doivent être identifiées. Dans la mesure du possible, les fonctions suivantes devraient être attribuées :

- le responsable sécurité de la compagnie ;
- le coordinateur de la sécurité des technologies de l'information ;
- le responsable pour chaque lieu distinct (département, filiale, détachement, etc.);
- le responsable des copies de sauvegarde ;
- le responsable de la gestions des renseignements personnels ;
- les personnes impliquées dans le processus de validation des procédures ;
- etc.

Une nouvelle fois, si la répartition des responsabilités est toujours considérée comme un gage d'assurance auprès des acteurs, elle dépend toutefois de la dimension de l'entreprise. Des regroupements sont donc en bien des cas envisageables.

► Les éléments à protéger

En deuxième lieu, il est capital de prévoir tant les éléments qui nécessitent une protection que les risques qui en découlent. Bien que tout ne puisse être prévu, il est recommandé au commerçant électronique de mettre par écrit les éléments pertinents. De cette façon, il pourra efficacement anticiper les incidents potentiels. Sans être exhaustif, les principaux risques concernent notamment :

- l'hypothèse de négligence ou de malversation d'un employé de l'entreprise : il s'agit, par exemple, d'un employé qui laisse son mot de passe sur un autocollant posé sur le coin de son écran ;
- le packet sniffing : il s'agit, par exemple, d'un tiers qui tente d'intercepter les mots de passe de personnes autorisées à l'aide d'un fichier qu'il a préalablement

introduit dans un endroit névralgique du système informatique sécurisé de l'entreprise ;

- l'accès des employés à des sites indésirables ou non sécuritaires : à cet égard, l'entrepreneur pourrait envisager de surveiller le trafic de son réseau (snooping) afin de vérifier la nature des sites Web consultés par le personnel et, le cas échéant, de bloquer l'accès aux sites indésirables. Les logiciels de surveillance de trafic, comme ONGuard Internet Manager, permettent de visualiser en direct un site consulté par un employé et d'en bloquer l'accès immédiatement. Ils permettent aussi de constituer une liste des sites qui ont déjà été consultés, de créer un fichier de sites indésirables et d'en interdire l'accès automatiquement ;
- la destruction et la modification de fichiers ou tampering et data diddling : il s'agit de formes diverses d'altération frauduleuse des données pendant leur stockage, leur traitement ou leur transmission, afin d'en fausser le sens, la valeur ou la destination. L'hypothèse extrême est celle d'un virus dont l'effet est de supprimer toutes les données contenues sur un disque. Le virus peut être déposé sur l'un des ordinateurs du réseau et être déclenché lors d'une manœuvre préprogrammée (réamorçage de l'ordinateur). C'est dans ce type d'intrusion que l'on peut placer le cas du « cheval de Troie », c'est-à-dire un fichier d'apparence anodine qui effectue une application malicieuse ;
- la dépersonnalisation ou spoofing : il s'agit d'un procédé visant à prendre l'identité d'un usager et, éventuellement, à lui donner celle d'une autre personne;
- l'encombrement ou jamming : il s'agit du type d'attaque qui a été particulièrement populaire à l'hiver 2000 sur plusieurs sites grand public américains;
- le décodage d'un mot de passe ou cracking passwords : action de passer outre un système de sécurité, notamment en trouvant une clé de chiffrement;
- l'exploitation des imperfections d'une structure de sécurité : à cet égard, l'architecture même de système de sécurité présente parfois ce type de défaut, notamment lorsque le langage JAVA est utilisé ;
- etc.

► Les procédures à suivre

En troisième et dernier lieu, l'entrepreneur devrait établir par écrit les procédures à suivre par les différents acteurs, c'est-à-dire par les acteurs propres à l'entreprise mais aussi par les acteurs qui lui sont extérieurs. En effet, ces derniers devraient connaître leurs obligations en cas d'intrusion non autorisée, particulièrement pour la prévention des attaques, leur détection et les facilités de réorganisation suite au piratage du réseau de l'entreprise. Les prochaines sections expliquent en détails les procédures à suivre. Parmi elles, se retrouvent principalement :

- le développement des politiques de sécurité et des procédures qui en découlent. Le commerçant prendra soin de gérer l'information à protéger, c'est-à-dire d'établir les différents niveaux de sécurité ainsi que les méthodes de protection relatives à chaque classe de documents ;
- la classification des activités sujettes à divulgation d'information sensible ou susceptibles de rendre le réseau interne vulnérable (intranet ou extranet). À cet égard, les informations sensibles devraient être protégées selon une procédure plus sécurisée ;
- l'identification des responsabilités de chaque intervenant ;
- l'établissement d'un plan de contingence, en précisant notamment ce qui constitue un incident à reporter, ce qui doit être enregistré, la procédure à suivre, etc.

- l'établissement des conditions de sécurité à respecter avec les partenaires tiers (fournisseurs, clients, etc.) et leur intégration contractuelle ;
- l'établissement des listes de vérification relatives aux respects des exigences demandées aux employés chargés du contrôle ;
- le regroupement des différents documents relatifs à la sécurité dans un guide facilement disponible pour les employés ;
- l'établissement des procédures pour rappeler les obligations de chacun, notamment quant aux conditions d'accès au réseau interne et externe. À ce titre, il est possible d'envisager un processus régulier de validation par l'employé d'un document récapitulant ses responsabilités et les conséquences consécutives à un manquement ;
- l'établissement d'une rotation d'entraînement des employés ;
- la création d'un dialogue quant aux solutions sécuritaires à apporter, et ce, à tous les niveaux ;
- le testage des procédures édictées ;
- l'établissement d'une liste des personnes autorisées à accéder à certaines classes de documents ;
- la vérification prédéterminée de l'adaptation des procédures de sécurité ;
- etc.

Sans doute le plus important des aspects à considérer lors de l'élaboration d'une politique de sécurité, l'organisation administrative requiert une implication de plusieurs couches de production. Cette considération nous amène à étudier la mise en place d'une sécurité organisationnelle sous l'aspect de la structure humaine.

La structure humaine

Le développement d'une conscientisation au sein de l'entreprise est nécessaire. Celle-ci doit être faite à chaque étape du processus de la gestion informationnelle. Tous les acteurs doivent comprendre qu'il ne sert à rien de veiller à la sécurité si celle-ci ne s'applique pas à l'ensemble de la chaîne informationnelle. Cette attention particulière survient d'abord chez les dirigeants ou les chefs de services, responsables du site Internet, qui financent le projet et qui prennent la décision de l'organiser sécuritairement. Elle se manifeste ensuite chez ceux qui s'occupent du contrôle de la sécurité, et enfin chez les employés chargés de l'application de la politique.

Une fois cet objectif atteint, les personnes impliquées dans l'élaboration de la procédure doivent spécifier précisément, selon le degré de sensibilité des informations à protéger, les obligations et responsabilités de chacun des acteurs concernés. Un entraînement régulier du personnel et des modalités de protection particulières doivent aussi être envisagés notamment en ce qui concerne le transfert ou le départ d'un employé ou d'un responsable. À cet égard, il est préférable de prévoir une clause spécifique dans un contrat de travail précisant les obligations que l'employé se doit de maintenir pendant et après l'échéance de son contrat. Cela peut requérir une adaptation des clauses de confidentialité existantes.

L'environnement physique

Il est faux de considérer que le changement de support du papier à l'électronique amène un désintéressement du caractère physique. L'information dématérialisée est toujours

située dans un lieu géographique peu importe le type d'opération effectué, que ce soit pour le simple stockage d'informations, pour la conclusion de contrats en ligne, pour le paiement ou pour la transmission de données. Un processus sécuritaire de gestion des informations dématérialisées doit donc prendre en compte la réalité physique.

La sécurisation de l'environnement physique prend appui sur trois thèmes majeurs que sont le stockage des données, leur accès et leur destructibilité.

Les modalités d'emmagasinage des données sont fondamentales pour l'établissement d'un environnement physique sécuritaire. En dépit de statistiques claires à cet effet, les atteintes à la sécurité de l'information sont en effet commises généralement par des personnes situées à l'intérieur de l'entreprise. Pour éviter ce type d'incidents, le stockage devrait en premier lieu être assuré dans un endroit pour le moins fermé, avec une serrure solide, des portes et des murs suffisamment résistants, un coffre-fort pour les données sensibles, un contrôle périmétrique (système d'alarme, patrouille, moniteur de télévision en circuit fermé, etc.), un contrôle des installations intérieures (interdiction d'accès après certaines heures, distinction des zones selon l'information qu'elles détiennent, etc.) et autres mesures de sécurité. Il existe d'ailleurs des normes internationales (ISO par exemple) et nationales (ceux de la GRC au Canada) très précises à ce sujet. En deuxième lieu, il est préférable de prévoir des procédures de vérification des performances des produits utilisés. Le responsable de la sécurité prendra soin de déterminer combien de temps l'information protégée est stockée et, à l'issue de sa perte d'intérêt, des modalités relatives à sa destruction, notamment après impression ou copie. À cet égard, il est inutile d'élaborer un cadre électronique de stockage sécuritaire mais ne rien prévoir une fois que l'information est imprimée. Il en est de même en ce qui concerne les copies, notamment pour les fins de transfert ou de transport. La facilité de reproduire les données dématérialisées ne devrait pas faire oublier que l'information n'est sécuritaire que si le contrôle s'exerce sur toutes ses reproductions. Notons d'ailleurs que des législations prévoient des modalités quant à la destruction de certaines données.

L'accès sécuritaire aux données protégées impliquent l'élaboration d'une procédure d'autorisation en ce qui concerne non seulement les lieux mais aussi certains dossiers. Tous seront accessibles seulement par des personnes déterminées et selon des conditions préétablies. Pour le moins, toute entreprise diligente devrait détenir une salle à accès limité, conformément aux conditions précitées, dans laquelle pourrait par exemple être localisé le serveur général, les installations d'alimentation électrique, un coffre-fort, mais également la salle de réception du courrier, etc. Également, les ordinateurs destinés aux communications extérieures et ayant notamment un accès Internet ne devraient pas être utilisés pour le stockage de données, pour le moins de façon permanente. Malgré l'apparente sécurité du réseau Internet, l'entreprise doit en effet distinguer les ordinateurs qui sont en ligne de ceux qui ne le sont pas. Dans le cadre du commerce électronique, il est toutefois fréquent que des données soient stockées sur un ordinateur connecté au réseau, notamment dans le cas d'un site Web transactionnel. Il est alors conseillé de mettre en place des mesures techniques telles que les coupes-feux (firewalls).

Enfin, le responsable de la sécurité doit considérer le caractère destructible des informations, quelles soient sur support papier ou sur support électronique. Il est donc nécessaire de se prémunir contre d'éventuelles dégradations naturelles (feu, inondations, fumée, tremblement de terre, etc.), de chocs divers ou d'explosions, de radiations électromagnétiques indésirables, etc. Ce type de protection existe déjà pour les documents papier et mérite souvent des adaptations minimes pour les documents électroniques. À cet

égard, il est parfois préférable de diversifier les sources de stockage, et donc de multiplier les lieux d'entreposage. Par ailleurs, l 'archivage électronique fait appel à une pluralité de moyens alors que de l'archivage de papier est généralement conditionné par l'unicité de l'original ou par l'existence d'un nombre limité de copies.

L'encadrement technique

La mise en place d'un encadrement technique sécuritaire concerne aussi bien les ordinateurs en tant que tel (hardware) que les logiciels qu'ils utilisent (software).

Relativement aux ordinateurs, les objectifs de sécurité s'articulent d'abord autour d'un inventaire de ceux qui sont utilisés ainsi que de leurs fonctionnalités respectives, notamment quant à l'accès aux réseaux extérieurs. Cet inventaire n'est utile que si une ou plusieurs personnes en sont les utilisateurs particuliers et que le mot de passe d'entrée n'est connu que de son utilisateur. Les numéros de série et de modèle, les fournisseurs ainsi que les dates de révision sont des informations pouvant être inventoriées. Des plans de contingence peuvent ensuite être mis en place afin de prévoir les modalités à suivre en cas de dysfonctionnement de l'un des ordinateurs. Sans reprendre les éléments physiques précédemment traités, il importe d'établir des techniques de verrouillage des ordinateurs, notamment des portables, en tenant compte que leur disque dur est amovible. Les politiques de sécurité devraient également prévoir un procédé de blocage des touches des claviers pour éviter que certaines d'entre elles ne soient activées par inadvertance. Cette considération est particulièrement utile dans le cadre du commerce électronique. On imagine les conséquences juridiques pouvant découler d'une commande envoyée à un fournisseur par le seul fait d'un livre tombé sur la touche « Retour ». Enfin, il importe de contrôler la bonne marche des ordinateurs selon une fréquence déterminée. Cette tâche consiste notamment à vérifier leur bon fonctionnement, leurs accès, l'absence de trace d'intrusion extérieure et les difficultés survenues. L'ensemble de ces informations devrait faire partie d'un registre enregistré et conservé pendant une période préétablie.

Quant aux logiciels, la protection qu'on doit leur accorder est du même ordre. Il faut toutefois ajouter certaines attentions supplémentaires en raison de leur reproductibilité, de leur amovibilité et de l'éventualité qu'ils soient installés sur un seul ordinateur et/ou accessible depuis le réseau de l'entreprise. Les systèmes de sécurité doivent par conséquent permettre une identification unique des usagers encore plus rigoureuse que pour les ordinateurs, surtout lorsqu'ils sont en réseau.

Les bases de données de l'entreprise doivent également être protégées. Dans le contexte du commerce électronique, ces dernières contiennent généralement des données relatives à l'inventaire de l'entreprise, aux transactions intervenues, aux commandes à effectuées ainsi que les informations personnelles des clients. Ces bases de données sont régulièrement ouvertes à une pluralité d'intervenants, voire même à l'ensemble des employés de l'entreprise. Une procédure de comportement est donc de mise, même si la mise en réseau de la base est effectuée de manière à préserver l'intégrité des données et à empêcher leur altération.

Notons enfin que l'ensemble de ces mesures de contrôle devrait être conforme aux règles applicables en droit du travail et notamment en ce qui concerne la vie privée des employés.

La communication

Tout site de commerce électronique comporte forcément un canal de communication vers l'extérieur. Il importe par conséquent de régir ce lien tout en assurant la conservation des données internes. Trois aspects peuvent être considérés, soit les techniques de contrôle des accès, les moyens de détection des intrusions et l'utilisation de procédés de chiffrement.

Les techniques de contrôle des accès telles que les coupes-feux (firewall), peuvent être d'un intérêt véritable pour le responsable d'un site Web marchant, notamment lorsque l'enjeu des transactions le justifie. Souvent, cette mesure technique est mise en place seulement pour des informations sensibles ou identifiées comme tel et non pour l'ensemble du site.

L'utilisation de moyen de détection d'intrusion non autorisée dans le système doit aussi être envisagée. Il s'agit d'un système de surveillance qui identifie les erreurs dans les applications de réseaux et dans les contrôles d'accès ainsi que les inconsistances quelconques susceptibles d'être découvertes. Pour des questions de preuve, il est fortement conseillé de garder pendant une période déterminée les enregistrements des informations recueillies par ces moyens de détection. Les vérifications et les tests du bon fonctionnement des canaux de communication représentent aussi des preuves de diligence très utiles dans l'hypothèse d'un éventuel différend.

L'utilisation de procédés de chiffrement dans le cadre de communication externe est un atout manifeste quant à l'intégrité et à la non altérabilité des informations et des documents transmis. Si cette technique peut être employée seulement pour certaines communications, soit plus à risque, soit plus sensibles, nul doute que la généralisation de ces procédés et la convivialité croissante des méthodes de chiffrement vont accroître leur utilisation. Notons néanmoins que certains États ont choisi de contrôler les instruments de cryptographie en raison des risques qu'ils comportent pour la sécurité nationale. Ainsi, les procédés de cryptographie sont assimilés à des armes et font partie de la liste des « biens et technologies à double usage », civil et militaire, soumis notamment à des contrôles à l'exportation en vertu de l'accord de Wassenaar de 1996. Plusieurs lois nationales tendent donc à restreindre l'utilisation d'outils de cryptographie robuste ou, du moins, à en permettre l'utilisation sous le contrôle de l'État.

Les opérations

Les considérations précédentes peuvent être appliquées différemment selon le type d'opérations effectuées. Dans le cas, par exemple, d'un contrat conclu électroniquement entre deux commerçants, les traces de l'entente doivent être conservées par chacune des parties, dont en premier lieu les éléments constitutifs du contrat, soit l'offre et l'acceptation. Ceci vaut dans l'hypothèse où ces éléments ont été clairement identifiés. En effet, il est souvent difficile de déterminer clairement leur présence en raison des nombreux échanges de documents et d'informations intervenant lors d'une entente dématérialisée. Il est donc nécessaire soit de reformuler le contrat, soit de préserver les traces pouvant indiquer l'existence d'un contrat. À cet égard, les accusés de réception électroniques sont des éléments de formalisme à privilégier. Il en sera d'ailleurs question dans le prochain chapitre consacré à la formation des contrats en ligne.