Comment sécuriser vos données et systèmes d’information ? | Denis JACOPINI

5

La cyberattaque, dont a été victime la chaîne TV5 Monde, puis ultérieurement le journal Belge Le Soir et d'autres médias, appelle à s'interroger quant à la sécurité des systèmes d'information.

La #sécurité des données informatiques représente un enjeu quotidien particulièrement important pour les sites d'e-commerce, les médias, les hébergeurs et les éditeurs de sites internet. Les banques et les compagnies d'assurances sont également concernées, en raison des multiples données qu'elles sont amenées à traiter dans le cadre de leurs activités.
La cyberattaque, dont a été victime la chaîne « TV5 Monde », puis ultérieurement le journal Belge « Le Soir » et d'autres médias, en témoigne et appelle à s'interroger quant à la sécurité des systèmes d'information, face au volume colossal des échanges de données sur les réseaux[1].
Outre les mesures préventives d'ordre technique à mettre en place, il est des mesures juridiques qu'il est hautement recommandé d'instaurer. Qu'à l'origine de l'attaque on identifie une faille interne à l'entreprise, ou externe (sous-traitant, hébergeur, etc.), il existe différents moyens juridiques à mettre en œuvre pour l'éviter. Les acteurs peuvent en effet être nombreux (éditeur, intégrateur, consultant, sous-traitant, prestataire, etc.) et la chaîne des responsables potentiels apparaît complexe.
Face au risque croissant de cyberattaque et aux enjeux du Big Data, il est indispensable de sécuriser l'ensemble des moyens techniques, humains et juridiques qui permettent de garantir la sécurité d'un système informatique.

1) La mise en place d'une stratégie en interne

a) En premier lieu, il est conseillé de procéder à un audit (juridique et technique) de sécurité du système d'information. L'objectif de cet audit sera de répertorier les points forts, et surtout les axes d'amélioration du système d'information dans son ensemble. Dans un monde en « hyper connexion » analyser une partie du système d'information n'a pas de sens car les risques peuvent venir d'un réseau ou d'une filiale non revus. Le but est de vérifier la sécurité du système afin d'identifier les mesures de réaction à une attaque, de tester un nouvel équipement, et surtout de mettre en place un planning de mise en conformité.
Les interventions liées aux opérations de maintenance corrective et évolutive doivent être régulièrement planifiées, notamment par l'application de correctifs de sécurité.

b) Ensuite, il est recommandé de rédiger une Charte de sécurité informatique, visant à sensibiliser chacun à la confidentialité et à l'importance de l'intégrité des données d'un système d'information. Une telle Charte représente une étape indispensable dans le processus de sécurisation des données. Elle doit viser les postes fixes, les mobiles, les tablettes, etc… et traiter, notamment, de la gestion des mots de passe, mais aussi de l'accès au réseau de l'entreprise depuis l'extérieur.

c) Soulignons qu'il convient d'instaurer une politique de gestion des mots de passe. L'utilisation d'un mot de passe dit « fort » est un élément fondamental dans la sécurisation d'un système d'information. Or, bien souvent, les mots de passe sont trop communs ou configurés par défaut. Il est donc essentiel de mettre en œuvre une politique de gestion des mots de passe afin de protéger tant l'utilisateur final, que le système d'information lui-même.
La surveillance des logs de connexion et de l'accès via des hotspot et/ou VPN est à encadrer également avec minutie.

d) Enfin, il est opportun de prévoir des clauses spécifiques dans les contrats de travail de l'ensemble des salariés au-delà des seuls administrateurs système, Directeurs des Systèmes d'Information (DSI).

2) Le développement d'une stratégie en externe

a) Avant tout accord, il convient de mettre en place une politique efficace de confidentialité en signant des accords de non divulgation (« Non-Disclosure Agreement ») avec l'ensemble de la chaîne des sous-traitants.

b) En parallèle de cela, il est nécessaire :
• de rédiger de solides contrats avec les différents prestataires techniques dont le non-respect sera sanctionné par des clauses pénales ;
• de vérifier régulièrement les contrats conclus avec les hébergeurs.

La rédaction des contrats informatiques nécessite en effet une expertise toute particulière. On pense notamment aux contrats de maîtrise d'œuvre, d'intégration, de sous-traitance, de licence d'utilisation, etc.
Pour ce qui concerne les obligations et garanties des parties, le contrat doit refléter la réalité des responsabilités. Le risque juridique est donc associé à la personne qui est effectivement responsable des traitements et des usages qui sont faits des données et des résultats.
L'application du régime du contrat de fourniture de prestations de services, complété par des obligations accessoires de surveillance et de respect de la confidentialité des données stockées, assure une protection optimale au bénéficiaire du service. Tout en servant les intérêts des utilisateurs, ce régime est également opportun à l'égard des prestataires car il correspond à leur nature juridique et à leur responsabilité sur le Web.

c) Il demeure indispensable de veiller au respect des recommandations de la CNIL. Il est nécessaire de procéder à toute déclaration requise en fonction de la nature des données et des modalités du traitement (déclaration simplifiée, déclaration normale, ou autorisation préalable) ; les formalités préalables étant allégées en cas de désignation d'un Correspondant Informatique et Libertés ou « CIL ».
Au sein de sa structure, ou en externe pour les petites structures, le responsable du traitement désigne une personne qui sera chargée de (i) tenir à jour un registre des traitements mis en œuvre au sein de l'organisme et (ii) veiller au respect des dispositions de la loi « informatique et libertés » au sein de l'organisme. Le CIL ainsi désigné peut être notamment être un salarié de la société, ou le conseil de cette société.

d) Le contrat doit également permettre la possibilité aux acteurs de la DSI d'auditer leur prestataire (droit d'audit). Cela permet de contrôler que les mesures contractuelles, par exemple sur la sécurisation de données, sur l'hébergement des données au sein de l'espace Européens, sont respectées.

e) Enfin, il est toujours possible de solliciter l'intervention de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI) qui veille quotidiennement au renforcement de la Cyber sécurité en accompagnant les entreprises par des actions de conseil, de politique industrielle et de réglementation.

3) En phase contentieuse

En cas de conflit, il est nécessaire de faire dresser des constats informatiques aux fins de préserver la matérialité de l'infraction et surtout de retracer l'origine de l'attaque ou de l'intrusion.
Par conséquent, la sécurité des données implique la mise en place d'une stratégie juridique renforcée, que ce soit tant au niveau des systèmes d'information que des réseaux de communications électroniques (mails et réseaux sociaux).

[1] En 1 minute, voici notamment ce qui s'échange sur la toile :
– 204 millions d'emails expédiés ;
– 1.875.000 likes sur Facebook ;
– 278 000 Tweets expédiés ;
– 694 445 recherches sur Google ;
– 70 noms de domaine enregistrés ;
– 13 000 applications téléchargées.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.journaldunet.com/solutions/expert/60588/cyberattaque–comment-securiser-vos-donnees-et-systemes-d-information.shtml