



GOVERNANCE DU SI

Quelle sécurité demain ?

L'industrie informatique vit une transition rapide avec l'omniprésence d'Internet et de ses multiples applications. Mobilité, Cloud, utilisation de données non structurées feront de l'informatique de demain un monde totalement différent de celui d'aujourd'hui. La sécurité et l'administration de cette « nouvelle informatique » va suivre ces nouvelles tendances. Au programme : le renforcement des éléments de gouvernance et la mise en œuvre de la sécurité comme un processus métier de l'entreprise.

La sécurité, dans laquelle il faut inclure les problématiques de conservation des données et de reprise ou de la continuité de l'activité, concentre toutes les peurs et toutes les inquiétudes. Lors de l'édition américaine de la RSA Conference, Art Coviello, patron de RSA, l'entité sécurité d'EMC, prônait la mise en place d'un Cloud de confiance. Depuis, les mauvaises nouvelles se sont accumulées, avec des

interruptions de services emblématiques sur le Cloud comme Amazon, Sony ou Blackberry. La société RSA a été elle-même victime d'une attaque ciblée d'envergure (lire l'article en page 36).

Si les causes en sont différentes, le doute est toujours là dans les esprits sur le Cloud, les services mobiles ou simplement en ligne. Un des enseignements à tirer de cet exemple reste que personne n'est infaillible et que malgré sa puissance de feu informatique et

son expérience non négligeable d'environnements complexes comme un Cloud, Amazon a été à la merci d'une erreur de configuration, donc d'une erreur humaine. En fait, la cause doit être un peu plus profonde puisque l'explication de l'incident tient sur un document de 25 pages au contenu très technique, et donc le plus souvent inaccessible au béotien ou à l'utilisateur lambda. La promesse d'entrer les enseignements et de revoir les processus avec un recours plus grand à l'automatisation sert de viatique à Amazon pour faire amende honorable. Éric Domage, analyste spécialiste de la sécurité chez IDC, expliquait récemment dans une interview aux *Échos* : « *Tout repose maintenant sur la sécurité des directions informatiques des entreprises. À elles d'améliorer l'encadrement et la gouvernance de leur SI pour faire face aux problèmes de sécurité.* »

Conformité ou sécurité ?

On peut définir la gouvernance comme l'ensemble des règles internes et externes à l'entreprise qui lui permettent d'exercer son activité à la fois dans le cadre légal mais aussi dans celui de son secteur d'activité tout en étant compatible avec la poursuite de ses objectifs. Cette définition n'est pas complète ni très académique mais s'approche beaucoup de ce qui se met en place en réalité. Luis Delabarre, de Trend Micro, estime que la gouvernance est un axe majeur. « *Il y a beaucoup de débats autour de cela et les questions sont présentes dans les appels*



d'offres. » Gilles Castéran, chez Arismore, explique que « la gouvernance, c'est aussi très opérationnel, même si c'est sur une plateforme de haut niveau et cela doit être comme cela pour créer un vrai échange entre ceux qui décident et ceux qui agissent. » Il ajoute : « c'est à ces conditions que la transformation peut s'effectuer et que peut se mettre en place une vue consolidée des risques et des performances. »

Le respect de la conformité et des normes en sont des aspects ainsi que la gestion des risques. Les outils de gestion de la conformité permettent d'assurer que l'entreprise a bien mis en place les outils et les procédures demandées par les autorités légales ou professionnelles. Cette mise en œuvre a pour but de dégager la responsabilité de l'entreprise. Il est cependant important de se poser la question, dans le cadre de la sécurité des systèmes d'information, si la conformité suffit pour apporter la sécurité. Ce ne semble pas souvent le cas. À mots couverts, les personnes interrogées lors de cette enquête ont bien souvent concédé que les deux n'allaient pas souvent de paire. Martin Roesch, chez Sourcefire, a été le plus net sur ce point lors d'un entretien sur les Assises de la Sécurité : « Une majorité de responsables de SI font de la conformité, peu font de la sécurité. » Jean-Claude Bellando, chez Axway, ajoute : « Normalement, cela va de pair. » Arnaud Cassagne, chez Nomios, constate de plus à nouveau des projets sur la norme PCI DSS depuis juin dernier.

Pourtant la conformité semble l'arme fatale pour obtenir des budgets et lancer des projets. Selon le secteur d'activité ou la sévérité des sanctions possibles, la conformité reste une grande pourvoyeuse d'opportunités. Elle

« Une majorité fait de la conformité, peu font de la sécurité »

Martin Roesch (Sourcefire)

peut de plus être un véritable levier de sensibilisation dans l'entreprise sur les questions de sécurité. Le point est d'ailleurs d'une telle importance que les fournisseurs intègrent directement les normes dans leurs produits. Chez Radware, la nouvelle appliance AMS (Attack Mitigation System) embarque des rapports sur la conformité à certaines normes dont PCI DSS mais aussi FISMA, HIPPA et GLBA.

Chez Wallix, la prochaine version 3 de son logiciel Admin Bastion embarquera les éléments pour répondre directement aux auditeurs des entreprises.

Cyrille Barthélémy chez Intrinsec, constate d'ailleurs que la démarche vers la conformité est largement simplifiée si des processus qualité de type ISO sont déjà en place dans les entreprises. D'ailleurs la démarche est assez similaire dans son cheminement.

Définir le niveau de risque acceptable

Le pendant de la démarche de gouvernance est de prendre conscience des risques et d'allouer les ressources là où elles sont nécessaires et non pour une sécurité totale de type château fort comme auparavant. Julien Steunou, en charge du conseil en sécurité chez BT France, explique : « Les entreprises vont vers le pilotage de la sécurité par les risques, ce qui est le fondement d'une bonne gouvernance de la sécurité. Cette démarche garantit que les moyens de sécurité sont alignés sur les enjeux de l'entreprise et non sur des aspects uniquement technologiques. La sécurité accompagne alors le business et vise à atteindre, pour chaque activité, le niveau de risque acceptable. Ce niveau de risque acceptable est défini par la direction générale et les besoins de conformité aux réglementations. De plus, une gouvernance basée sur un système de



management de la sécurité de l'information (SMSI) efficace permet de produire simplement les éléments prouvant la conformité. »

Dans le domaine, les tests de vulnérabilité sont un premier niveau. De nombreuses solutions existent sur le marché. La plus connue en France est Qualys, mais d'autres offres commencent à pointer leur nez comme la solution WebSure proposée par Athena Global Services pour l'audit de site web et qui s'appuie sur le moteur d'Acunetix. Il est possible de les combiner avec des tests d'intrusion pour mesurer les risques. La plupart des intégrateurs spécialisés dans la sécurité ont mis cette prestation à leur catalogue comme GFI Informatique ou Intrinsec que nous avons déjà cités. Des spécialistes comme NES sont aussi sur ce créneau.

Il faut cependant bien se rendre compte que l'approche par les risques s'appuie sur des compromis dont les compromis budgétaires. L'ensemble de ces éléments « gouvernance, conformité et risques » sont au cœur aujourd'hui des questions de sécurité et sont les briques essentielles pour apporter confiance et visibilité dans les environnements émergents comme le Cloud.

Ces briques mises en place devraient ensuite s'automatiser et apporter la possibilité de traiter la sécurité à l'égal d'un processus métier dans l'entreprise. Les grandes entreprises françaises sont déjà sur ce chemin. Il est cependant encore long, même si des fournisseurs commencent à communiquer sur ce thème. Il devrait devenir le sujet le plus important aux alentours de 2015. Cyrille Barthélémy confie cependant que « le message n'est pas ultra neuf. Je ne suis pas très convaincu du côté novateur depuis le temps que l'on parle des processus d'amélioration continue ». ■



« Il y a beaucoup de débats autour de la gouvernance et les questions sont présentes dans les appels d'offres »

Luis Delabarre (Trend Micro)