Innovation technologique et protection des SI : une opportunité à saisir pour les DSI ?

Chronique de Julien Bizjak
Abington Advisory 23/05/16 17:54

Les ruptures technologiques en cascade que nous vivons depuis les dernières décennies favorisent l'accroissement des vulnérabilités et cyberattaques. Dans ce contexte, la protection des systèmes d'information est plus que jamais critique.

Notre société profite depuis plusieurs décennies de mutations technologiques profondes visant à simplifier notre quotidien et celui des entreprises. Ces transformations s'accompagnent d'une multiplication exponentielle des vulnérabilités au sein des SI. L'évolution des technologies vers les objets connectés (Internet of things) amplifie encore ce phénomène : des attaques peuvent désormais viser l'intégrité humaine.

Dans ce contexte, pour conserver leurs avantages concurrentiels sur des marchés instables, les entreprises doivent s'approprier ces mutations technologiques et se protéger de manière adaptée.

Record des cyberattaques

Les ruptures technologiques en cascade que nous vivons depuis les dernières décennies favorisent l'accroissement des vulnérabilités et cyberattaques.

L'étude 2015 de l'éditeur mondial de solutions de sécurité CheckPoint en témoigne :

142 millions de nouveaux virus identifiés en 2014, soit une augmentation de plus de 70% par rapport à 2013,

80% des entreprises ont subi un incident de fuite de données en 2014, soit plus du double qu'en 2013, et principalement d'origine interne.

Tout porte à croire que les chiffres 2015 suivront les mêmes tendances.

Ces derniers mois, des cyberattaques ont été très largement relayées par les médias, dont :

Dans le domaine criminel : près d'un milliard de dollars volé en 2 ans à une centaine de banques réparties sur une trentaine de pays (dont en France) par une coalition criminelle (« Carbanak »)

Dans le domaine terroriste : piratage des comptes Twitter et YouTube du commandement militaire américain au Moyen-Orient, ou encore l'attaque contre TV5 Monde en avril 2015

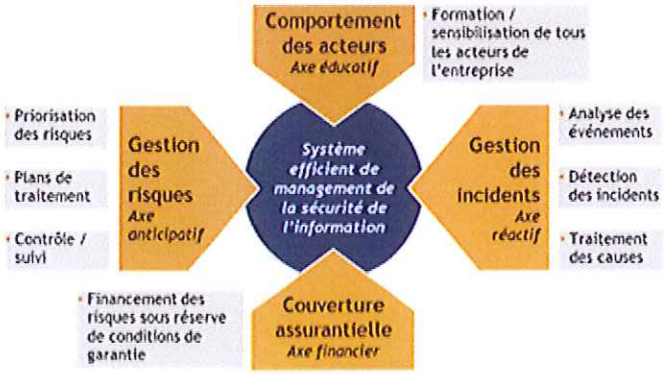
Attention toutefois à ne pas céder à la panique (voir le syndrome FUD : Fear, Uncertainty and Doubt) comme ce fut le cas en 2014 de BAE Systems ou bien encore de TF1.

Comment se protéger ?

Les avantages concurrentiels des entreprises étant de plus en plus déterminés par leur capacité à s'approprier l'innovation technologique, la protection de leur SI est une condition nécessaire pour leur pérennité et leur développement.

Pour être efficace, cette protection doit s'appuyer sur une posture complète mobilisant un système efficient de management de la sécurité fondé sur un principe d'amélioration continue. Cette posture complète et efficiente combine quatre axes complémentaires :

4 axes complémentaires de la sécurité des SI.



Un axe anticipatif via l'évaluation, la priorisation, le traitement des risques de sécurité et une organisation de contrôle et de suivi de conformité. Cela suppose de cartographier les actifs critiques de l'entreprise (services, infrastructures, compétences, documents papiers, fournisseurs...) pour cibler les risques majeurs grâce à l'utilisation d'une méthode adaptée.

Un axe réactif pour détecter et traiter les incidents de sécurité (vol de données...) grâce à un système complet et centralisé de corrélation des événements du SI. Capable d'analyser également les signaux faibles, ce système repose sur une organisation et des procédures partagées, notamment en matière de confinement d'incident et de conservation des preuves.

Un axe financier visant à transférer les impacts financiers et coûts induits par une attaque (par exemple : la charge

de travail nécessaire au redémarrage d'une activité suite à un sinistre ou bien encore les impacts financiers d'un vol de données). Cela suppose de maitriser en amont les risques associés, et leur évolution, afin de les financer auprès d'un assureur via des indemnisations sous réserve de conditions de garantie.

Un axe pédagogique visant à faire évoluer les comportements en sensibilisant tous les acteurs de l'entreprise aux enjeux de sécurité. Cet axe est essentiel pour la mise en œuvre de la protection des SI et nécessite un processus de sensibilisation s'appuyant sur des relais internes (par exemple : via les réunions d'équipes animées par les managers) pour pérenniser les messages et règles à appliquer.

Une fonction Sécurité diffuse et intégrée au sein de l'organisation de l'entreprise

Le responsable de la sécurité des SI (RSSI), dont le rattachement hiérarchique dépend de la maturité de l'entreprise en la matière, pilote la feuille de route Sécurité et le tableau de bord associé déclinant les objectifs stratégiques de l'entreprise (financiers, image de marque...) et résultant des quatre axes décrits ci-dessus. Le RSSI n'agit pas seul, mais en chef d'orchestre mobilisant des relais internes au sein des directions métiers (Production, Vente, Finance, RH, Achats, Juridique...) et de la direction des SI (exploitation, développement, architecture/urbanisation, gestion de projets...). Cette organisation compose la fonction sécurité des SI et requiert des budgets à répartir entre les projets et l'exploitation courante du SI selon les risques associés et les contraintes pour l'entreprise.

Afin de répondre aux attentes des clients internes de la DSI (« time to market », qualité de service ...) et contribuer à améliorer la qualité des services fournis, la fonction Sécurité du SI ne doit pas constituer une contrainte rallongeant les délais des projets (ou bloquant même certains projets) mais doit travailler en collaboration avec les équipes opérationnelles afin de faciliter leurs activités. Elle peut notamment :

Être un facilitateur auprès des métiers, notamment en promouvant et sécurisant les nouvelles technologies et nouveaux usages (digital) en lien avec les équipes de la DSI,

Fournir aux équipes projets de la DSI, un formulaire en ligne d'expression des besoins métiers de sécurité et suivant le cycle de vie des projets,

Fournir aux équipes de production de la DSI, des scripts automatisés d'installation sécurisée des systèmes et des bases de données (durcissement).

Ainsi, la protection des SI constitue une condition désormais nécessaire pour la pérennité et le développement des activités métiers des entreprises ainsi qu'une opportunité forte offerte aux DSI pour améliorer l'industrialisation et la qualité de services fournis à leurs clients.