

Cahier du manager

forum du manager

La sécurité informatique

Objectifs et enjeux pour l'entreprise

L'évolution du nombre de partenariats et l'amélioration de la performance de l'entreprise reposent sur l'accès facile à l'information pertinente. Dans un tel contexte, il est primordial d'identifier les sources de l'information et d'en maîtriser l'accès ! Débat...

L'accès à l'information est la source de développement des entreprises. Aussi, la contrainte du temps et le souci de la productivité poussent ces dernières à partager de plus en plus d'informations avec leurs différents partenaires et fournisseurs. Par conséquent, la sécurité informatique devient l'une des préoccupations majeures de l'entreprise. Car, les systèmes d'information non sécurisés sont exposés à diverses menaces qui peuvent nuire à la crédibilité, l'image et le rendement de l'entreprise. En fait, le rôle de la sécurité est d'éviter toute altération de l'information et de maîtriser l'accès des différents utilisateurs. Pour faire face à ces difficultés, les entreprises s'engagent dans une politique de sécurité qui assure la confidentialité, l'intégrité et la disponibilité de l'information. Ce sujet, qui préoccupe tant les entreprises, a fait l'objet du débat, lors du dernier forum du manager. Lors de la réunion, plusieurs questions ont été soulevées: Quels sont les objectifs fondamentaux de la sécurité? Quels sont les aspects d'une telle politique? Et quelle est la culture de l'entreprise par rapport à une telle démarche? Selon Yassir Jorio, vice-président du pôle IT de Finatech, «80% à 90% des cas de piratage et des fuites des systèmes d'information sont faits en interne. Et 43% des entreprises à l'international considèrent la sécurité de l'information comme une partie



Zainab Outana
Essor

intégrale de la gestion de l'information». Soucieuses des répercussions de l'insécurité sur les données des systèmes d'information, les entreprises déploient des efforts considérables pour une meilleure gestion de risque. Objectif: promouvoir une culture de la confidentialité liée aux droits des utilisateurs.

Conditions préalables

Avant de procéder à la sécurisation d'un système d'information, il est essentiel de distinguer les différents objectifs de la sécurité. Ces derniers constituent les critères à même d'évaluer la sécurité au niveau de l'entreprise, telles que la confidentialité, l'intégrité et la disponibilité. Ces dernières permettent de préserver les données et les ressources matérielles et logicielles. Elles garantissent également la circulation des informations entre les différents partenaires de l'entreprise et ce, en toute sécurité. La confidentialité consiste à assurer l'accès aux sources de l'information partagée aux seules personnes autorisées. Car, selon Diyaa-edinne Najjar, architecte réseaux et serveurs à SiWay Networks, société de e-commerce et de gestion des systèmes d'information, «l'accès à l'information est un privilège. Donc, il faut s'assurer des personnes auxquelles l'information est divulguée!». L'intégrité, quant à elle, permet de vérifier si les données du système d'information ne sont pas altérées ou volontairement modifiées par des per-

sonnes non autorisées. Par conséquent, l'intégrité est un élément essentiel car elle garantit l'exactitude et la totalité des données. En effet, «l'intégrité consiste à ce que les données résidentes ou transmises soient exemptées de toute modification non autorisée», explique Yassir Jorio. La disponibilité, quant à elle, veille à ce que les informations soient accessibles aux utilisateurs autorisés, au moment voulu. «Quand il y a un problème de sécurité comme une intrusion ou bien un sabotage, cela affecte la disponibilité de l'information aux utilisateurs autorisés», affirme Yassir Jorio. Cependant, «la traçabilité est un autre élément qu'il faut bien prendre en considération au niveau de la sécurité de l'information», selon Karim Hamdaoui, directeur général de LMPS consulting, société spécialisée dans la sécurité de l'information, la gestion des risques et la conformité. Car, explique-t-il, «elle permet de tracer les accès aux données du système d'information pour être sûr que l'information existe». Alors, avant de tenter de se protéger, il faut d'abord s'assurer de la prise en compte de ces objectifs lors de la mise en place du projet de sécurité.

Nécessité absolue d'une politique de sécurité

Le management de la sécurité est généralement conditionné par l'esprit de volontarisme, supposé influencer l'attitude du personnel de l'entreprise et ce, à tous les niveaux. Cependant, l'élaboration et la gestion de la sécurité doivent être initiées par la direction, car cela concerne tous les uti-

« Pour 43% des entreprises à l'international, la sécurité est une partie intégrale de la gestion des systèmes d'information. »

declare Yassir Jorio, Vice-PDG du pôle IT services, Finatech



forum du manager

management

marketing

ventes

ressources humaines

finances

Juridique

technologie

lisateurs du système. Yahya Arroubat, responsable du service support de la direction des systèmes d'information de la bourse de Casablanca, insiste, en effet sur le fait que, « pour que la politique de la sécurité soit bien menée au niveau de l'entreprise, il faut un engagement financier et moral de la direction ». Et il ajoute que « la préservation de l'information est d'une grande importance pour le business et l'image de l'entreprise. Aussi, le management de cette dernière doit soutenir le volet de la sécurité à travers des audits et des qualifications ». De plus, il est important que l'audit sur la sécurité soit réalisé en externe par des établissements spécialisés, afin de pouvoir maximiser le contrôle des systèmes d'information. C'est ce que soutient Karim Hamdaoui, qui estime que « l'audit des systèmes d'information doit se faire en externe et non en interne! ». Le système de sécurité doit être basé sur des mécanismes de contrôle, qui assurent que les utilisateurs possèdent seulement les droits qui leur ont été accor-



Yassir Jorio
Finatech

dés par l'entreprise. Mais, il faut prendre en considération que le système de contrôle ne doit pas empêcher les utilisateurs d'accéder à des informations qui leur sont nécessaires. Pour ce faire, il est essentiel de sensibiliser le personnel sur l'importance de la sécurité pour l'entreprise, avant de procéder au lancement du projet. « Il ne suffit pas de disposer de bons outils technologiques, encore faut-il sensibiliser les collaborateurs quant aux enjeux majeurs de la sécurité », souligne Tawfik Benkirane, responsable des méthodes qualité et sécurité informatique à la Société Générale. « Il faut maîtriser les risques et prendre les décisions en tenant compte des moyens de l'entreprise. Mais, il ne faut pas négliger que l'être humain est un élément très complexe dans cette équation! », appuie Yahya Arroubat. Tout type de sabotage ou d'intrusion du système d'information peut avoir un impact négatif sur l'image de l'entreprise. Cela peut également mener à des conséquences non négligeables sur le rendement de l'organ-

me. « Les risques liés à l'image de l'entreprise sont importants. Il faut savoir que les failles au niveau de la sécurité du système d'information nuisent à la crédibilité de l'entreprise », affirme Yassine Naim, programme office manager à M2M Group, leader mondial dans le secteur des solutions de gestion de la transaction électronique sécurisée et de la dématérialisation de flux. L'entreprise doit davantage accorder de considération aux mesures de sécurité relatives aux systèmes d'information, via d'importants budgets. En effet, selon Tawfik Benkirane, « il est important d'investir dans le volet de la sécurité. Ce service doit être considéré comme une nécessité pour l'entreprise et non pas comme une contrainte ». Et Yassir Jorio de conclure qu'« à l'international, un bridge (une faille) de sécurité en interne coûte annuellement 3,4 millions de dollars aux entreprises ».

Pour une sécurité maximale

Afin de promouvoir une vraie politique de sécurité et de contrôle, il est nécessaire de cibler les différents aspects relatifs à ce projet.

Cahier du manager



Karim Hamdaoui
LMPS Consulting



Mohamed Amine Hajami
GFI Maroc



Ahmed El-Abbadi
Algortech



Nicolas de la Fortelle
SiWay

Il faut, tout d'abord, « identifier le besoin et faire le bon dosage pour les risques », selon Mohamed Amine El Hajami, responsable du projet Oracle middleware à GFI Informatique, société de services et des technologies de l'information. La détection des vulnérabilités et la maîtrise des failles au niveau du matériel, du logiciel et du personnel accédant à l'information en interne et en externe, sont autant d'éléments importants pour promouvoir une vraie politique de sécurité au sein de l'entreprise. Aussi, il faut distinguer deux manières d'héberger les services de sécurité au sein de l'entreprise. L'hébergement en interne, qui consiste à rattacher le service de sécurité à la direction des systèmes d'information et l'hébergement en externe, qui consiste à considérer le service de sécurité comme un département indépendant, pas nécessairement installé dans le même bâtiment que l'entreprise. Dans les deux cas, le responsable dudit service doit directement traiter avec la direction générale. Le choix de l'héberge-

ment du service de sécurité doit être fonction de la taille et des besoins de l'entreprise. « En 2006, Bank of America a affronté une grande faille au niveau de la sécurité. Ils ont alors séparé la sécurité de la direction informatique », relate Yassir Jorio. Pour maximiser le contrôle de la sécurité des systèmes d'information au Maroc, l'engagement de l'Etat et des ONG est indispensable. Une campagne de sensibilisation auprès des collaborateurs pourra également mener à une vraie démarche de changement au niveau de la culture de sécurité des systèmes d'information dans le pays. Cette sensibilisation semble nécessaire car, déplore Yassir Jorio, « certains collaborateurs circulent librement munies de clés USB contenant des données confidentielles de l'entreprise ». Une prise de conscience de l'importance de la sécurité informatique est indispensable, avant qu'une catastrophe n'exige, pour tous, une réforme d'urgence. ■

Par Zainab Outana



Yassine Naim
M2M Group



Diyaa-eddine Najjar
SiWay



Taoufik Benkirane
Société Générale



Prochain Forum du Manager
Réussir la dématérialisation,
pour une meilleure fluidité, traçabilité et productivité.

Le jeudi 15 juillet 2010 à La centrale des salles - Casablanca

Pour vous inscrire: www.sp.ma