→ RISQUE

La sécurité informatique: priorité du secteur bancaire

La sécurité informatique est passée au premier plan des priorités affichées par les responsables techniques du secteur bancaire. La réponse à la montée des vulnérabilités s'organise progressivement: elle ne peut être que systémique si elle veut être efficace.

JEAN-MARIE CHAUVET
General Partner LC Capital Dassault Développement.

LA CONJUGAISON des événements liés au terrorisme, du poids croissant des réglementations, et de la montée des atteintes à la fiabilité et à la confiance dans les communications électroniques a placé la sécurité informatique au premier rang des priorités des directeurs des systèmes d'information du secteur bancaire. Citons, parmi les nouveaux sujets d'actualité:

→ La gestion de crise et la coordination des différents acteurs et des réseaux informatiques de la banque et de la finance;
→ La lutte contre de nouvelles formes de fraude (*clearing*, vol d'identité...);
→ Les risques contractuels de l'infogérance;
→ Les usages frauduleux du courrier électronique, les attaques du réseau de télécommunication, les virus informatiques, les intrusions...

Les résultats du récent *2004 E-Crime Watch Survey* conduit par le *CERT* et la revue *CSO Magazine* sont alarmants: 70% des sociétés interrogées signalent un nombre croissant d'attaques informatiques. Le coût des failles de sécurité est estimé à 666 millions de dollars pour 2003 et à plus d'un milliard pour 2004.

LE COÛT DES FAILLES DE SÉCURITÉ EST ESTIMÉ À 666 MILLIONS DE DOLLARS POUR 2003 ET À PLUS D'UN MILLIARD POUR 2004.

engendrées par ces défaillances et, pour les autres, les sous-estiment. Enfin, 30% ignorent si les attaques sont perpétrées de l'intérieur ou de l'extérieur de l'entreprise; pour celles qui le savent, 71% des attaques sont externes et 29% internes.

Une lutte sans fin

Quel que soit l'effort technique investi à contrer les nouvelles menaces, pare-feux et filtres, surveillance des réseaux et des flux, la lutte contre leur complexité croissante est sans fin. Et plus la complexité s'accroît, plus nombreuses sont les failles de sécurité.

La réponse efficace à ces menaces et à leurs effets réels est alors *systémique*.

Elle prendra non seulement plus de temps à s'établir et, paradoxalement, se heurtera à court terme à une certaine résistance. La raison en est que le moteur de cette réponse n'est plus à chercher au laboratoire de R&D mais bien au conseil d'administration ou à la direction générale.

Au stade actuel, cette solution repose en effet sur la restauration d'un régime de *responsabilité*: rendre l'industrie du logiciel et des réseaux comptable de la sécurité des produits qu'elle conçoit et commercialise.

La sécurité informatique, même si elle comporte une composante technique indéniable, est essentiellement un problème de personnes et de responsabilités. Les organisations s'attaquent à cette question comme aux autres questions de responsabilité: en termes de gestion de risque. Payer plus que le coût d'une solution pour la sécuriser ensuite n'a pas de sens économique.

De même payer la compensation d'un dommage n'a pas de sens si le coût de sa prévention en est inférieur. Le secteur bancaire fait aujourd'hui le minimum économiquement rationnel pour équilibrer les coûts et bénéfices de ce risque sécurité. Comme le risque augmente, mais lentement, les dépenses de sécurité augmentent, mais lentement.

Renforcer les responsabilités

Par le même raisonnement, les éditeurs de logiciels dépensent aujourd'hui relativement peu pour la sécurité de leurs produits: il n'ont pas d'incitation économique à la faire.

Dans le même temps, le nouveau régime doit permettre le transfert de responsabilités. Ainsi les directions générales peuvent faire appel aux compagnies d'assurance, dont c'est le métier, et transformer un risque à coût variable en dépense à montant fixe.

A partir d'une certaine masse critique de contrats, le jeu naturel de la différenciation des primes d'assurances suivant le niveau de sécurité devient pour ces compagnies un puissant levier d'orientation de l'industrie: incitation économique a évaluer au mieux le risque pour les acheteurs (le coût de leurs primes en dépend), incitation économique à prendre en compte le coût «plus le coût de l'assurance» dans la commercialisation pour les éditeurs (leur succès en dépend).

LE CHEMIN EST ENCORE LONG, MAIS LES PREMIERS SIGNES ENCOURAGEANTS ÉMERGENT AUJOURD'HUI SUR LA ROUTE D'UNE RÉPONSE SYSTÉMIQUE AU PROBLÈME DE LA SÉCURITÉ INFORMATIQUE.

La standardisation des contrats d'assurance «sécurité»

Enfin, ce régime encourage naturellement la généralisation de dispositifs de réduction de risques.

Les éditeurs ont une incitation réelle à employer des méthodologies de développement et de test plus fiables, et le secteur bancaire à normaliser les processus de protection, de détection et de réponse. Cette généralisation entraîne la standardisation des contrats d'assurance «sécurité» et la diminution globale des coûts.

Le chemin est encore long, mais les premiers signes encourageants émergent aujourd'hui sur la route d'une réponse systémique au problème de la sécurité informatique. ■