ABSTRACT A LA PUBLICATION CNRS :

VERS LA MAITRISE DE LA SECURITE DES SYSTEMES D'INFORMATION ET DE COMMUNICATION

CONTEXTE

Le développement des Systèmes d'Information et de Communication (SIC), aussi bien dans le secteur privé que dans le secteur public, a conduit le Management à se préoccuper de la sécurité de l'information. Des premières mesures efficaces ont été appliquées, allant de la sensibilisation du personnel au renforcement de la sécurité des locaux, en passant par l'amélioration de la sécurité du fonctionnement des applications, jusqu'à la fourniture de services critiques aux clients internes et externes.

L'ouverture des SIC aux réseaux et aux services Internet a accéléré ce mouvement, en mettant en évidence la nécessité de revoir le plan de réduction des risques attachés aux SIC. Des audits de sécurité complétés par des tests d'intrusion ont permis d'identifier les vulnérabilités majeures. Ces revues ont donné lieu, d'une part, au renforcement des systèmes de contrôles d'accès à l'information, et d'autre part, à la mise en place des systèmes de surveillance du fonctionnement des SIC et des systèmes de détection et de correction automatique des incidents répertoriés.

Le Risk Manager, en étroite collaboration avec le RSSI (le Responsable de la Sécurité des Systèmes d'Information), analyse les nouvelles menaces et recherche les parades adaptées. Le rôle du RSSI a été renforcé, lui permettant de proposer et de mettre en place des mesures préventives et correctives, réduisant les risques encourus par les SIC.
Ces actions d'amélioration ont constitué des progrès importants, aussi bien dans les domaines organisationnels que dans les domaines techniques.

A l'occasion du passage à l'An 2000 et de la mise en place de l'Euro, le patrimoine applicatif des organisations a été revu et épuré, d'une part, des composants obsolètes, et d'autre part, des identifiants et des mots de passe inscrits en clair dans les programmes, et enfin, des applications et des modules qui n'étaient plus utilisés ou qui pouvaient constituer de véritables brèches au cœur des SIC.

La charge importante de mise à hauteur des applications informatiques, engendrée par le passage à l'Euro, a souvent empêché les Directions des SIC de mener une réflexion globale sur les processus contribuant à la maîtrise de la sécurité des SIC. Les nouvelles exigences des métiers et les opportunités technologiques font apparaître de nouveaux risques majeurs et nécessitent une nouvelle analyse des menaces et des parades.

Deux axes d'amélioration des processus de sécurité sont à privilégier par le Management :
1. La prise en compte systématique de la sécurité dans la conduite des projets, par la définition et l'intégration des actions de sécurité dans les jalons de développement des projets, pour mieux réduire les risques inhérents aux nouvelles exigences de sécurité.
2. Le renforcement des actions de sécurité dans le fonctionnement quotidien des environnements de production, pour mieux assurer la continuité des services rendus aux clients internes et externes.

FONDEMENTS DE LA SECURITE DES SIC

Il y a lieu de distinguer :

- La sécurité de l'information
- Le contrôle des accès à l'information

- L'architecture sécurisée des SIC
- Les critères d'évaluation de la sécurité des SIC

La sécurité de l'information :

La sécurité de l'information requiert les exigences suivantes :

- La confidentialité : l'information n'est accessible qu'aux personnes habilitées.
- L'intégrité : l'information est exhaustive, exacte et résulte d'activités autorisées.
- La disponibilité : l'information est accessible en continu, sans interruption ni dégradation de service.
- L'auditabilté et la traçabilité des traitements effectués sur l'information ou des opérations réalisées à partir de l'information.

Le Contrôle des accès à l'information

Le contrôle des accès à l'information consiste à empêcher son utilisation non autorisée ou non conforme aux règles de sécurité définies. Le contrôle des accès est assuré par l'application de 3 mécanismes :

- L'identification : indiquer au système de contrôle l'identité de l'utilisateur demandant l'accès à l'information.
- L'authentification : vérifier que l'identité de l'utilisateur est correcte. Le renforcement de l'authentification des utilisateurs et de l'authentification des messages reçus par un utilisateur est quelquefois nécessaire lorsque les exigences d'intégrité sont très fortes.
- L'autorisation : accorder ou refuser à l'utilisateur des droits d'accès à l'information. .

L'architecture sécurisée des SIC

Il s'agit de sécuriser l'infrastructure technique et les moyens de production informatique tels que :

- Les serveurs, les systèmes d'exploitation, les logiciels associés et les outils de production,
- Les bases de données,
- Les réseaux internes et externes et les équipements associés.

Il convient également de sécuriser les applications et les services mis en production, aussi bien ceux qui sont développés en interne que ceux qui sont acquis à l'extérieur sous la forme de progiciels intégrés. Le niveau de sécurité de ces applications et services doit être conforme aux exigences de sécurité définies par les métiers.

Les critères d'évaluation de la sécurité

Les critères d'évaluation des SIC prennent de plus en plus en compte les besoins réels et potentiels des métiers exercés par l'utilisateur final et des applications critiques correspondantes. On peut citer quelques modèles d'évaluation :

- EFQM (European Foundation for Quality Management), qui propose un modèle général de gestion de la qualité, permettant de mieux situer les actions de sécurité.
- Les modèles CMM et SPICE, qui permettent aux organisations de s'inscrire dans un processus d'amélioration continue de la sécurité en définissant les étapes nécessaires à la maîtrise de la sécurité.
- ITSEC (Information Technology Security Evaluation Criteria), qui propose différentes classes de sécurité pour les systèmes critiques.
- Les critères européens, qui propose les Critères Communs (CC) normalisés ISO.

PROCESSUS DE MAITRISE DE LA SECURITE DES SIC

Il y a lieu de distinguer :

- Le modèle global des processus de maîtrise de la sécurité des SIC.
- Les rôles et les responsabilités associés au modèle global des processus de maîtrise de la sécurité.

Michel PRIE et Ladan PEGAH

Césys