Méthodologie de sécurisation d'un campus

■ Edouard GHERARDI, gherardi@u-cergy.fr
Université de Cergy-Pontoise

L'audit de la sécurité des systèmes d'information de l'université de Cergy-Pontoise a été réalisé au moyen de la méthode MARION 95 du Club de la Sécurité des Systèmes d'Information Français (CLUSIF). Toutefois, les limites de cette méthode sont apparues rapidement. Néanmoins les adaptations nécessaires ont été effectuées pour son application à un établissement d'enseignement supérieur multi-disciplinaire, réparti sur huit sites distants. Sa mise en œuvre a permis d'élaborer un schéma directeur de la sécurité des systèmes d'information, ainsi que la réalisation concrète de la première phase et une partie de la deuxième phase du plan d'action.

■ Méthode d'audit

L'audit pour la sécurité des systèmes d'information de l'université de Cergy-Pontoise (UCP) a eu lieu d'octobre 1998 à mars 1999. Il s'est appuyé sur la méthode MARION 95 du Club de la Sécurité des Systèmes d'Information Français (CLUSIF).

Cette méthode de management de risques se déroule en quatre phases :

- Phase 0 - Initialisation :
  - Sensibilisation, définition du champ, convention et métriques, création d'un comité de pilotage.
- Phase 1 - Analyse des vulnérabilités :
  - L'analyse des vulnérabilités repose sur un questionnaire, structuré en vingt-sept facteurs caractéristiques, regroupés en six chapitres :
  - Appréciation générale de la sécurité (101-103).
  - Les facteurs socio-économiques (201).
  - Principes généraux de la sécurité informatique.
  - Sécurité physique (301-307).
  - Sécurité générale (308-311).
  - La sécurité des matériels et logiciels de base (401-403).
  - La sécurité de l'exploitation (501-505).
  - La sécurité des études et réalisations (601-604).
  - Chaque facteur aborde un ou plusieurs thèmes. Par exemple, le premier facteur « organisation générale » est divisé en sept thèmes (organigrammes hiérarchiques et fonctionnels, comité sécurité, étude de vulnérabilité, etc.). Chaque thème est noté de zéro à quatre et la note est pondérée. Une pondération, établie statistiquement par le CLUSIF en fonction du secteur d'activité, est affectée également à chacun des facteurs.
- Phase 2 - Analyse des risques :
  - Elle permet de construire des scénarios de risques, en fonction des vulnérabilités détectées dans la phase précédente. Cette phase utilise la base de connaissances Menaces MARION. On évalue pour chaque scénario son impact et sa potentialité.
- Phase 3 - Plan d'action :
  - Le plan triennal est établi à partir des simulations reposant sur un algorithme d'optimisation sous contraintes. Les solutions retenues donnent lieu à la rédaction du schéma directeur, qui fixe plannings et budgets, ainsi que l'organisation de la sécurité (structures, procédures, contrôles, tableaux de bord, etc.).

■ Application

Difficultés

Inhérentes à la méthode MARION : Coût élevé de la méthode, qui ne nous a pas permis de faire l'acquisition de la base de connaissances Menaces, ni du moteur d'évaluation des scénarios. La méthode convient mieux pour des entités monolithiques et très centralisées. Pour un campus comme l'UCP, réparti sur huit sites distants et possédant une certaine autonomie, la méthode MEHARI du CLUSIF (ou d'autres) aurait été plus adaptée.

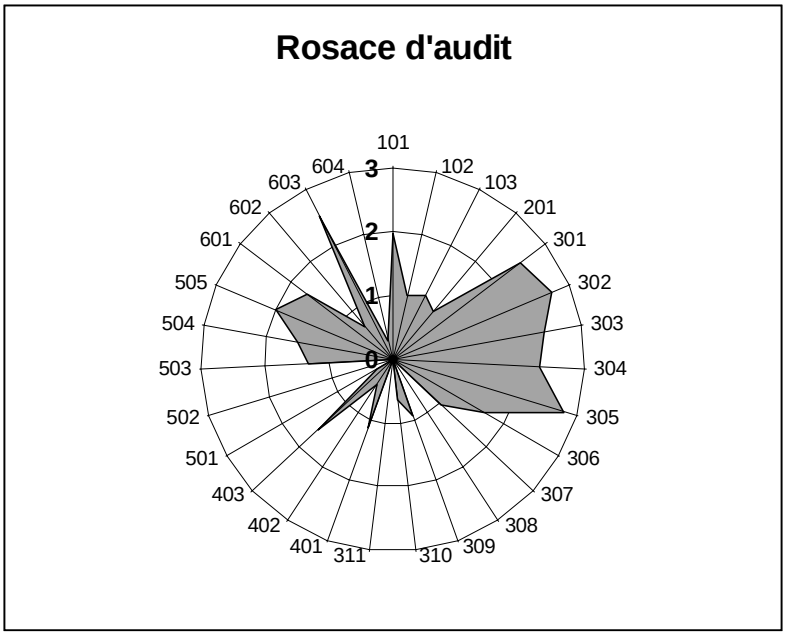
Liées à l'organisation : Une seule personne pour réaliser l'audit, en un temps relativement court.

Difficultés d'ordre général : il est parfois très difficile d'obtenir des informations. Ce qui ne manquera pas d'avoir des répercussions, lors de la mise en place du plan d'action.

Analyse des vulnérabilités

Réalisée à partir des réponses au questionnaire et des entretiens avec des responsables (administrateurs de bases de données ou de serveurs, chefs de services, agent comptable, etc.).

Cette phase terminée, nous obtenons une rosace d'audit très explicite, qui se présente ainsi : **Plus sa surface est importante et bien répartie, plus les moyens mis en place pour la sécurité sont forts et homogènes. Plus elle se rapproche du centre, plus l'établissement est vulnérable.**



La méthode MARION fournit des tables techniques permettant de calculer et de représenter le positionnement de la sécurité existante par rapport aux conséquences possibles en :

- Disponibilité.
- Intégrité.
- Confidentialité.

Et par rapport aux causes possibles en :

- Accidents.
- Erreurs.
- Malveillance.

L'échelle va de zéro à quatre. A zéro, les conséquences sont très faibles et les causes possibles rares. A quatre, les conséquences sont extrêmement graves. On considère que la note 2 marque la frontière entre risques simples (<2) et risques majeurs (>2).

Valeurs obtenues pour l'université de Cergy-Pontoise :

	Disponibilité	Intégrité	Confidentialité	Accidents	Erreurs	Malveillance
NOTE	**2,69**	**2,74**	**2,55**	**2,55**	**2,76**	**2,75**

Toutes les valeurs sont supérieures à 2,5. Cela ne peut que renforcer la première analyse et amène le constat simple : L'université est extrêmement exposée à tout type d'attaques.

Analyse des risques

Les risques matériels accidentels

L'étude des vulnérabilités a montré que cet aspect est l'un des points forts de l'université : La sécurité physique est correctement assurée sur tous les sites. Aucune implantation n'est en zone dangereuse (inondation, tremblements de terre, etc.). L'implantation sur huit sites réduit grandement le risque d'un sinistre total. Les principaux serveurs et équipements sont protégés par onduleurs. Enfin, les systèmes de sauvegardes existent. Sauf qu'aucun circuit de distribution des sauvegardes n'est en place et que tous les sites ne disposent pas de coffre ignifugé. Compte tenu de ces éléments, on peut considérer ce type de risque comme peu probable.

Les erreurs

On peut circonscrire le risque d'erreurs lié à la conception d'applications à la création, actuellement en cours, du serveur intranet de l'université. Les applications de gestion comportent toutes des contrôles programmés, qui réduisent les possibilités d'erreurs. De plus, des contrôles supplémentaires sont effectués par les gestionnaires et les responsables de services. Le risque d'erreurs est là aussi minimum.

Les vols et sabotages matériels

Nous l'avons vu, la protection physique des personnes et des biens est bonne. Toutefois, il est difficile, surtout sur une telle superficie de bâtiments, de réduire complètement ce risque. Beaucoup de facteurs entrent en jeu et augmentent la probabilité de risques (erreur humaine, organisation, protection des locaux, etc.).

Les fraudes et sabotages immatériels

Il s'agit là du risque le plus important, de par l'impact qu'il peut avoir et également de par sa probabilité d'advenir, quasi certaine. A tel point qu'il s'est déjà produit, plusieurs fois. Il n'y a pas encore eu de fraudes en ce qui concerne les applications de gestion. Il n'est pas exclu qu'il y ait eu des tentatives de l'extérieur, les outils manquaient pour s'en assurer. En revanche, il est certain que l'université a été victime de fraudes sur certains autres serveurs. Ces attaques venaient de l'extérieur et certaines ont abouti (découverte de mots de passe). L'établissement a subi, en novembre 98, une attaque provoquant l'écroulement du réseau (dénis de service). En janvier 99, l'établissement a été utilisé comme relais, par un pirate, pour attaquer un site canadien.

L'indiscrétion et les détournements d'informations

Les fonctionnaires sont tenus à un devoir de discrétion et les détournements d'informations bien que difficilement contrôlables paraissent peu probables. Toutefois, l'absence de rigueur et l'étourderie amènent à commettre des erreurs. Les exemples les plus courants étant de donner son mot de passe à un collègue ou de l'écrire sur un papier collé sur l'écran ou encore d'utiliser un fichier de données nominatives à d'autres fins sans en avertir quiconque. Il y bien d'autres exemples.

Adaptations

Le questionnaire a été adapté, ainsi que les facteurs de risques, afin de mieux coller à la réalité (ex.: le facteur assurances n'a pas vraiment de signification pour l'établissement).

Utilisation d'un tableur pour l'exploitation du questionnaire d'analyse des vulnérabilités.

Ne disposant pas de la base de connaissances Menaces, nous avons bâti les scénarios de risques sur nos propres connaissances en la matière. Cette phase d'analyse a par conséquent été allégée (pas de consolidation).

■ Plan d'action

Prévu, pour plus de souplesse, en trois phases, plutôt que sur trois ans, il porte dans sa partie matérielle sur les réseaux d'une part et sur les outils de protection d'autre part. La volonté politique très forte d'établir la sécurité des SI de l'établissement a permis d'engager la première phase et une partie de la seconde.

Pour la partie réseaux : Mise en place d'un routeur central et d'équipements CABLETRON, permettant la commutation sur les principaux sites et la création de réseaux virtuels sécurisés (VLAN Securefast).

En ce qui concerne les outils de protection : Mise place d'un garde-barrière, d'un antivirus central et de trois sondes de détection d'attaques (sur les serveurs de gestion).

Coûts TTC : 1re phase 800 KF, 2e phase 1400 KF, 3e phase 720 KF.