Université du Québec à Montréal

Rapport d'activité de synthèse

Présenté comme exigence partielle
de la Maîtrise en informatique de gestion

par

Marc-André Léger

Un processus d'analyse des vulnérabilités technologiques comme mesure de protection contre les cyber-attaques.

Juin 2003

Remerciements

Je remercie mon directeur de recherche, monsieur Guy Bégin, mon père Paul-André Léger, ingénieur retraité, et mon épouse Hélène Blouin, pour leur soutient tout au cours de la réalisation de ce travail.

Je remercie les employés et participants du Technocentre Régional de Montréal , messieurs Gilles Blanchette, Jean-Pierre Cordeau, Pierre Desautels, André Paradis et Dino Lolli.

Ce rapport de travail de synthèse est dédié à la mémoire de ma mère, Suzanne Blain Léger, à qui mon épouse a promis que je terminerais ce que j'ai commencé...

4**Table des matières**

Liste des abréviations

CAI	Commission d'accès à l'information du Québec
CAIDA	the Cooperative Association for Internet Data Analysis.
CERT	Computer Emergency Response Team Coordination Center du Carnegie Mellon University, Pittsburg, Pennsylvania, USA
CHU	Centre Hospitalier Universitaire
CSI	Computer Security Institute, San Francisco, CA, USA
CVE	Common vulnerabilities and Exposures (liste de vulnérabilités technologiques publiées sur le site Internet http://cve.mitre.org
DBA	Database administrator, administrateur de bases de données
EPR	Electronic patients records, dossiers médicaux sous forme numérique
GO	Giga Octets
GTQ	Le Groupe des télécommunicateurs du Québec, regroupement de fournisseurs de services de télécommunication pour le Gouvernement du Québec
iCLSC	application de gestion de dossiers développés pour les CLSC
Itsec	IT security, sécurité des technologies de l'information
JDBC	Java Database Connector,
LDAP	Lightweigt Directory Access Protocol
Loi sur l'accès	La Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès, L.R.Q., chapitre A-2.1
LSSS	La Loi sur les services de santé et les services sociaux (LSSSS, L.R.Q., chapitre S-4.2)
MSSS	le Ministère de la santé et des services sociaux
NVAS	Network Vulnerability Assessment Software
NIST	National Institute of Standards and Technology, USA
OPHQ	l'Office des personnes handicapées du Québec

RAM	Random access memory, mémoire vive
RAMQ	la Régie de l'assurance maladie du Québec
RH	Ressources Humaines
RRSSS	Régie Régionale de la Santé et des Services Sociaux de Montréal-Centre
RTSS	le réseau de télécommunication sociosanitaire
SI	Système d'information
TCR	Technocentre Régional
TCN	Technocentre National, situé à Québec
TI	technologie de l'information
VPN	Virtual private network

Liste des tableaux

Liste des figures

1 Introduction

Lors d'un discours présenté à l'ouverture de la conférence RSA 2002, l'aviseur spécial du Président Bush en matière de cyber-sécurité[1], Richard Clarke, a réitéré que dans la foulée des événements du 11 septembre 2001, les organisations doivent donner à la sécurité informatique une très haute priorité [Poulsen, 2002]. Il a précisé que dans le futur il est probable que des terroristes chercheront à exploiter des faiblesses dans les systèmes informatiques.

> *"This industry runs the same risk that the aviation industry ran. For years, people in the aviation industry knew that there were security vulnerabilities. They convinced each other and convinced themselves that these vulnerabilities would never be used."*

Une étude, menée par le Computer Security Institute auprès de praticiens de la sécurité des technologies de l'information dans diverses organisations américaines, confirme que l'augmentation des menaces liées à la cyber-criminalité et à l'usage non autorisé de systèmes d'information ne montre aucun signe de ralentissement [CSI, 2002]. De 3 734 incidents en 1998, le CERT Coordination Center de l'université Carnegie Mellon a répertorié 82 094 incidents en 2002. Les pertes économiques qui découlent de la cyber-criminalité et de l'usage non autorisé des systèmes d'information ne cessent d'augmenter. Pis encore, la majorité des cyber-attaques réussies via le réseau InterNet ont profité des vulnérabilités qui avait déjà été identifiées [SANS, 2002].

Prenons comme exemple le virus informatique Code Red, la vulnérabilité exploitée a été initialement identifiée en mai 2001. Ce virus a infecté environ 359 104

[1] White House's Special Advisor for Cyber Security

ordinateurs la seule journée du 19 juillet 2001 sur une période d'environ 13 heures [CAIDA, 2002(1)][Moore, 2002][Berryman, 2002][Martin, 2001]. En tout, plus de 700 000 serveurs ont été infectés [iDefence, 2002].

Le 25 janvier 2003 à 5h30 GMT le virus SQL Slammer a frappé. La vulnérabilité dont tirait profit ce virus avait été identifié le 17 mai 2002, soit plus de quinze mois plus tôt [Microsoft, 2002][CERT, 2002][CERT, 2003]. Le virus a infecté plus de 75000 ordinateurs, 90% de tous les ordinateurs infectés, en dix minutes. Entre autre, SQL Slammer a affecté des guichets automatiques de la Banque Canadienne Impériale de Commerce qui n'ont pas fonctionné une partie de la journée du 25 janvier.

Selon la base de données du Computer Security Division du National Institute of Standards and Technology (USA), en janvier 2002 il y avait 3 526 vulnérabilités identifiées et au début janvier 2003, on en comptait 5 356 [NIST, 2002]. Plusieurs de ces vulnérabilités ont le potentiel d'être exploitées.

Des analyses ont révélé que les administrateurs des serveurs ne prennent pas de mesures correctives pour s'immuniser [Berryman, 2002][Martin, 2001]. Que se soit par manque de temps ou par inhabilité à évaluer correctement le risque, les administrateurs rendent les systèmes d'information vulnérables à des cyber-attaques comme Code Red ou SQL Slammer.

Il y a sur le marché des produits et des services qui permettent d'assister les administrateurs dans l'identification des vulnérabilités des systèmes d'information dont ils ont la responsabilité [CSI, 2002(1)][Forristal, 2001][CSI, 2002(1)]. Avec de tels outils, un administrateur pourra être en meilleure posture pour identifier plus efficacement des situations à risque. L'administrateur aura alors l'opportunité de prendre des actions correctrices. Il évitera des impacts négatifs sur la disponibilité de

ses systèmes d'information ou des impacts sur la qualité des données qu'ils contiennent.

1.1 Problématique

Les chercheurs impliqués dans ce travail de synthèse, comme praticiens des systèmes d'information de gestion impliqués dans des projets en matière de sécurité de l'information, ont observé que bien des organisations n'ont pas de processus d'analyse des vulnérabilités. Pis encore, peu d'organisations semblent s'y intéresser. En démontrant l'efficacité d'un processus continu d'analyse des vulnérabilités comme mesure de protection contre les cyber-attaques, nous souhaitons en démontrer l'intérêt. Ainsi nous souhaitons amener les praticiens et les organisations à se questionner sur la faisabilité et la rentabilité de mettre en place un tel processus. Éventuellement ce questionnement pourra emmener des investissements en technologies et en ressources humaines dont bénéficieront directement les chercheurs impliqués.

Comme beaucoup d'organisations publiques et privées, le Technocentre régional de Montréal souhaite remplir son mandat tout en offrant une infrastructure qui dispose d'un niveau de sécurité adéquat. Il n'a pas nécessairement une structure organisationnelle formelle pour traiter des aspects de la sécurité sous sa responsabilité. Comme c'est le cas pour de nombreuses organisations, surtout depuis les événements du onze septembre 2001, le Ministère de la Santé et des Services sociaux place en haute priorité la gestion de la sécurité dans ses réseaux informatiques. En effet, le TCR souhaite se munir d'outils, de processus et de ressources dans un contexte de l'évaluation du risque. Par cette évaluation du risque le TCR sera en mesure d'évaluer les menaces à son environnement et ainsi mettre en place les structures appropriées pour efficacement gérer le risque. Une des options disponibles aux organisations est la mise en place d'un processus continu d'analyse des vulnérabilités. La mise en place d'un tel processus est d'ailleurs recommandée

par plusieurs normes internationales et *Best Practices*.. Les principaux obstacles observés à la mise en place de ce processus dans une organisation sont la justification de l'investissement, la difficulté à en évaluer les bénéfices pour la sécurité de l'organisation et les changements organisationnels requis pour en maximiser l'efficacité.

1.2 Question de recherche

Un processus formel d'analyse des vulnérabilités technologiques est-il une mesure de protection efficace contre les cyber-attaques ?

1.2.1 Questions secondaires

1. Quels sont les processus organisationnels du TCR qui seront affectés par la mise en œuvre d'un processus d'analyse des vulnérabilités ?

2. Comment les extrants (informations et les rapports) d'un processus d'analyse des vulnérabilités doivent-ils être utilisés au TCR ?

1.3 Définitions

Un **processus** est définit comme une série d'actions consécutives ayant un lien logique entre elles visant à obtenir un résultat prédéterminé [Davenport, 1990].

Les **systèmes d'information** sont un élément des technologies d'une organisation. Ils comprennent un ensemble organisé d'équipements, de réseaux, de programmes, logiciels, progiciels, codes et de données, utilisés par une organisation dans le cadre de son exploitation et de sa gestion.

Les **systèmes d'information de gestion** sont un segment particulier des systèmes d'information qui procurent aux gestionnaires d'une organisation des informations qui sont utiles, soit directement ou indirectement, dans la gestion des divers éléments de l'organisation.

La **sécurité de l'information** est définie comme l'ensemble des actions et des procédures conçues pour prévenir, avec un niveau de certitude démontrable, la divulgation, le transfert, la modification ou la destruction non autorisée, volontaire ou accidentelle de données [Schumacher, 1997]. Les principaux objectifs de la sécurité de l'information sont :

- la confidentialité des données;
- l'intégrité des données;
- la disponibilité des données;
- la non répudiation des transactions;
- l'authentification des utilisateurs;
- l'authentification de l'origine des données; et

- le contrôle des accès.

La **confidentialité** identifie la sensibilité de l'information ou des biens à une divulgation non autorisée, évaluée à l'aide d'une cote de classification ou d'une désignation correspondant au niveau de dommage produit advenant une divulgation non autorisée.

L'**intégrité** est l'exactitude et l'intégralité des renseignements et des biens et l'authenticité des transactions.

La **disponibilité** est l'accessibilité d'un système d'informations ou des données qu 'il contient, au moment opportun, pour exécuter certains processus.

La **non-répudiation** des transactions ou l'**irrévocabilité** des transactions fait référence à la pérennité et la traçabilité des transactions.

L'**authentification des utilisateurs** définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, l'identité d'un utilisateur d'un système d'information.

L'**authentification de l'origine des données** définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, la source d'une donnée stockée dans un système d'information.

Le **contrôle des accès** comprend l'ensemble des mécanismes de contrôle et de journalisation (log) de l'utilisation d'un système d'information ou des données qu'il contient.

Nous définissions comme **conditions de base** en matière de sécurité (*baseline*) le profil de sécurité établi ou les conditions de sécurité déterminées à un moment donné.

Une **vulnérabilité** est un état dans un système d'information qui, s'il était exploité, permet [Schumacher, 1997] :

- de divulguer des données (atteinte à la confidentialité);
- de modifier des données (atteinte à l'intégrité);
- de nuire à la disponibilité des données;
- de répudier des transactions;
- de falsifier l'authentification des utilisateurs ou de l'origine des données; et
- d'éviter le contrôle des accès.

Une **vulnérabilité technologique** est une vulnérabilité dont l'origine ou la nature est directement relié aux éléments technologiques d'un système d'information (systèmes d'exploitations, logiciels, processeurs, équipements périphériques, interfaces d'entrée ou de sortie, etc.).

L**'analyse des vulnérabilités** consiste à observer, dans un processus formel, les vulnérabilités technologiques d'un système d'information.

L'**impact** est le résultat, l'effet ou la conséquence d'un événement, d'une action ou d'une situation sur une autre. Le résultat de l'exécution d'une vulnérabilité technologique ou de l'exploitation d'une menace est son impact.

L'**impact négatif net** est la somme de tous les impacts ayant une incidence directe ou indirecte négative sur le plan économique. Cet impact négatif est généralement exprimé sous la forme de sommes d'argent ou de pertes économiques.

Une **menace** consiste en une situation ou une condition avec le potentiel de compromettre la sécurité de l'information. Tout acte ou événement pouvant avoir

l'une ou plusieurs des conséquences suivantes : divulgation non autorisée, destruction, enlèvement, modification ou interruption de renseignements, de biens ou de services de nature délicate, ou blessures corporelles est une menace. Une menace peut être délibérée ou accidentelle [GRC, 1994]. La présence d'une vulnérabilité technologique, connue ou inconnue, est une menace.

L'**évaluation de la menace** consiste en l'évaluation de la nature, de la probabilité et des conséquences d'actes ou d'événements susceptibles de mettre en péril des biens ou des renseignements de nature délicate.

Le **risque** est l'impact négatif net résultant de l'exploitation d'une menace en considérant sa probabilité et ses impacts [GRC, 1994].

Les **mesures de protection** sont les éléments, les outils ou les processus mis en place pour réduire le niveau d'exposition, mitiger les conséquences d'une vulnérabilité technologique, contrer une menace ou solutionner un problème de sécurité particulier. En général, des mesures de protection pertinentes et bien utilisées réduisent le risque.

L'**évaluation des risques** est l'évaluation de la probabilité qu'une menace ou une vulnérabilité technologique soit exploitée, compte tenu de l'efficacité des mesures de protection existantes ou proposées.

L'**évaluation des menaces et du risque** consiste à observer, dans un processus formel, la relation entre la menace et le risque pour en évaluer la probabilité [GRC, 1994]. Cette analyse aidera l'organisation à déterminer les mesures de protection disponibles et prendre des décisions concernant la pertinence de leur mise en place.

Une **cyber-attaque** est définie comme l'exploitation d'une menace par l'intermédiaire des systèmes d'information ou de réseaux de télécommunications, tel que le réseau InterNet [Smith, 2002]. Une cyber-attaque pourra compromettre l'atteinte d'un ou de plusieurs des objectifs de sécurité de l'organisation.

Nous définissons comme **cyber-crimes** une cyber-attaque dans le but de commettre un méfait, une fraude ou un acte illégal [Smith, 2002].

2 Méthodologie

Pour ce travail de synthèse nous avons utilisé une méthodologie de type recherche-action. Certains chercheurs pensent que la recherche-action constitue un excellent moyen de développement et d'appropriation des technologies par les organisations [Baskerville, 1999]. Les quatre principales caractéristiques de la recherche-action sont:

- elle vise à accroître la compréhension d'une situation sociale avec une emphase sur la nature complexe des comportements;
- elle assiste dans la résolution d'une problématique existante tout en permettant l'avancement de la connaissance scientifique ;
- c'est un processus de réflexion en équipe qui permet l'avancement des connaissances de tous les participants;
- elle est particulièrement pertinente pour la compréhension du changement dans les systèmes sociaux [Hult, 1980].

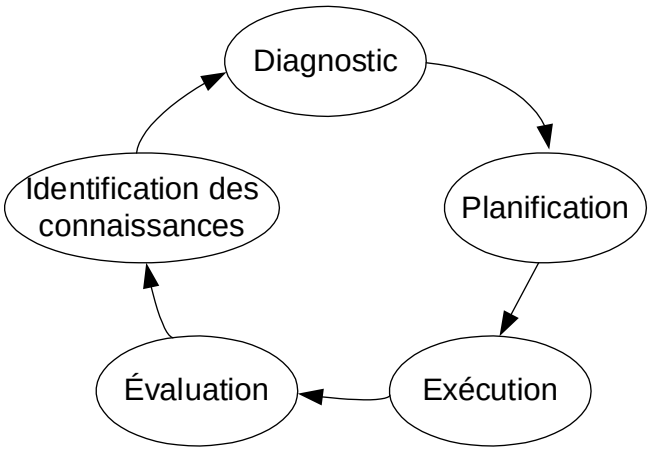

Figure 1 : méthodologie de recherche-action

Selon cette méthodologie, l'appropriation du changement s'effectue à travers une démarche itérative de changement planifié, tel que présenté à la figure 1. Elle comprend les phases suivantes [Baskerville, 1999] :

- Diagnostic ;
- Planification ;
- Exécution ;
- Évaluation ;
- Identification des connaissances.

Ce processus d'appropriation autogéré intègre une série d'activités susceptibles de faire naître un meilleur alignement entre la technologie et les autres éléments de l'organisation. L'expérimentation sociale des technologies devient un facteur de l'accroissement de la richesse collective et de la qualité de vie à travers de nouveaux modes d'accès communautaires au savoir [Harvey, 1997].

2.1 Limites

Lors de la proposition de recherche, il fut proposé de compléter trois cycles de la méthodologie en fonction de trois équipements ciblés. En réalisant trois cycles nous souhaitions démontrer qu'il y a un lien de cause à effet entre les résultats du processus d'analyse des vulnérabilités et le niveau de certitude de l'organisation par rapport aux objectifs de sécurité de l'information. Les équipements ciblés furent déterminés d'un commun accord entre les chercheurs et le TCR, soit :

- un serveur IntraNet Linux / Apache;
- un serveur Lotus Notes; et
- un serveur de base de données Oracle.

Dès le début de la mise en œuvre du travail de synthèse, le Coordonnateur de la sécurité du réseau du Ministère de la Santé et des Services Sociaux, monsieur Éric Dallaire, a demandé au chercheur principal des modifications à la proposition de travail de synthèse. Il a, entre autre, demandé qu'une analyse de la nature délicate des équipements ciblés soit effectuée. De plus il a été proposé de procéder avec un plus grand niveau de détail dans l'analyse des menaces et des risques que ce qui avait été envisagé lors de la proposition initiale. Il apparaît que d'augmenter le niveau de détail dans l'analyse d'un équipement augmente significativement la valeur pour l'organisation de l'extrant.

L'exécution du travail de synthèse avec la méthodologie choisie demande une participation active du chercheur principal et des participants. Dans le cadre de ce travail de synthèse il fut difficile de procéder au rythme envisagé lors de la proposition initiale. Le principal obstacle fut la difficulté à trouver des créneaux horaires disponibles de tous les participants impliqués. Bien qu'il fut possible de compenser par l'utilisation du courrier électronique, le volume important d'informations que chaque participant devait consulter afin d'arriver à des consensus sur les différentes étapes a rendu la tâche ardue aux participants. Ces praticiens ont des responsabilités opérationnelles.

Au cours de la réalisation du premier cycle de recherche il est apparu que la pertinence des apprentissages du travail de synthèse est très significative pour l'organisation. Le TCR n'ayant pas de processus formel d'analyse des menaces et des risques ni de processus d'analyse des vulnérabilités, il apparaît que l'amélioration du niveau de la sécurité de l'information procuré par une analyse des menaces et des risques à elle seule est très significative. Relativement, l'amélioration du niveau de la sécurité de l'information procurée par un processus d'analyse des vulnérabilités est moins significative. Ainsi il semble nécessaire d'évaluer la pertinence des deux éléments d'analyse du risque et des vulnérabilités ensemble comme catalyseur pour

l'amélioration de la position de l'organisation. Cette analyse des deux éléments conjointement sur trois cycles de recherche-action dépasse largement les exigences du programme de la Maîtrise en Informatique de Gestion. Il n'y a aucune indication que les résultats obtenus après trois cycles auraient plus d'intérêt pour l'avancement du domaine.

2.2 L'application de la méthodologie dans le projet

Le principe d'appropriation du changement à travers la démarche itérative de la méthodologie de recherche-action a été observé tout au long du travail de synthèse. Dès le début de l'exécution du travail, nous avons procédé à l'examen du contexte organisationnel et au diagnostic de la situation, que nous avons documenté avec l'aide des membres de l'organisation ciblé. La phase diagnostique de la méthodologie couvre le diagnostic initial et une partie de l'analyse de l'élément, phase initiale du processus d'analyse des menaces et des risques. Nous avons ensuite planifié un certain nombre d'actions, telles l'analyse des menaces et des risques et l'analyse des vulnérabilités, que nous avons ensuite exécutées dans la phase d'exécution de la méthodologie. À cette étape, nous avons produit les extrants principaux du point de vue de l'organisation. Une fois les résultats obtenus, nous les avons analysés dans le contexte de l'organisation (phase d'évaluation) avec celles-ci puis d'un point de vue plus théorique (phase d'identification des connaissances). L'ensemble de ces tâches et la relation entre la méthodologie et les étapes du travail de synthèse sont illustrés sur la figure 2.

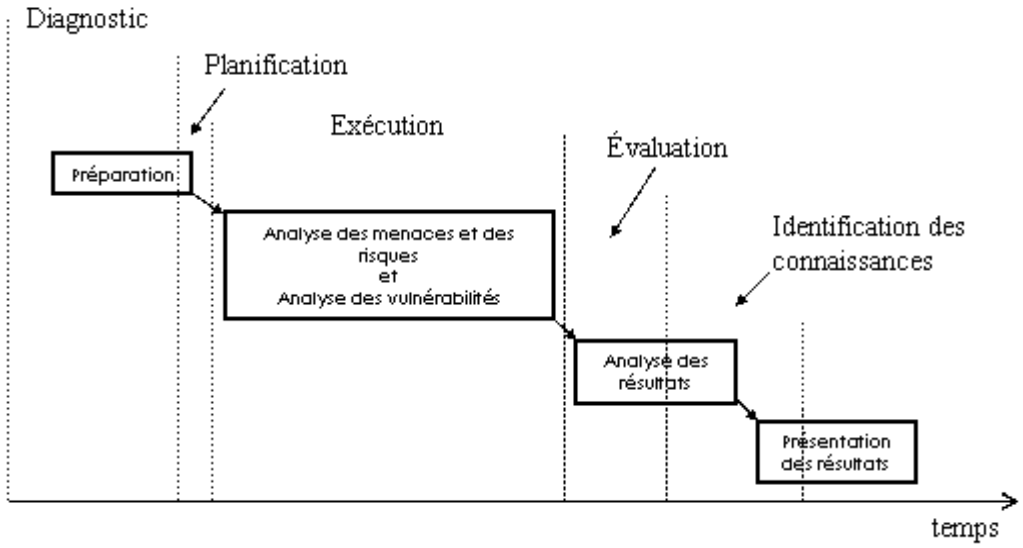

Figure 2 : la méthodologie dans le projet

Les différentes étapes du travail de synthèse sont décrites plus en détails dans les chapitres suivants. Une fois la méthodologie définie et le lien avec les activités identifié, nous avons réalisé un échéancier de projet avec l'aide du progiciel Microsoft Project. Nous avons débuté en travaillant avec Gilles Blanchet, Chef Développement et Déploiement, Secteur des Systèmes et des Technologies de l'Information, Régie Régionale de Montréal-Centre, afin :

- De valider les principales activités proposées ;
- De réviser la cédule de projet ;
- D'identifier les principaux participants à la réalisation des activités ;
- De démarrer le travail de synthèse.

Nous avons démarré le travail de synthèse avec la phase de diagnostic.

3 Contexte organisationnel

Lors de la première phase de la méthodologie, la phase de diagnostic, nous avons identifié et défini la situation que l'organisation souhaite changer. Dans cette phase, les chercheurs et les participants de l'organisation ont interprété de façon holistique l'ensemble des éléments qui définissent le phénomène organisationnel complexe qu'est la sécurité d'un système d'information. Ce diagnostic a permis l'élaboration d'un certain nombre d'hypothèses de travail sur la nature de l'organisation et la problématique de la mise en place d'un processus d'analyse des vulnérabilités de même que son impact sur le niveau de sécurité perçu dans l'organisation. Afin de réaliser cette phase, des recherches ont été effectuées dans la littérature courante et sur les sites Internet d'organismes et ministères impliqués[2]. Nous avons recueilli les principaux éléments d'information dans un document qui a été envoyé aux participants au projet du TCR. Essentiellement ce document comprenait les informations contenues au chapitre 3, soit la description de l'organisation et de son mandat, les principaux enjeux pour celle-ci et un aperçu du contexte légal dans lequel l'organisation évolue. Par la suite nous avons procédé avec l'analyse des menaces et des risques (Chapitre 4) et l'analyse des vulnérabilités (présentée au chapitre 5).

3.1 Le TCR et le RTSS

En 1994, dans la foulée de réformes structurelles dans le secteur de la santé au Québec, le Ministère de la santé et des services sociaux (MSSS) a créé le réseau de télécommunication sociosanitaire (RTSS). Ce réseau étendu est le principal véhicule d'échange d'information entre les établissements du réseau de la santé et des services sociaux. Il permet de desservir les établissements de santé et de services sociaux, les

[2] Principalement : http://www.msss.gouv.qc.ca/f/index.htm , http://www.msss.gouv.qc.ca/rtss/ , http://www.msss.gouv.qc.ca/rtss/

dix-huit régies régionales, la Régie de l'assurance maladie du Québec (RAMQ), l'Office des personnes handicapées du Québec (OPHQ), le MSSS, ses organismes conseil et les autres organismes relevant du Ministre. Les informations susceptibles d'être échangées entre les établissements sont d'ordre clinique, administratif ou financier [COSIS, 1999].

Situé sur l'avenue Christophe-Colomb dans l'arrondissement Plateau Mont-Royal de la ville de Montréal, le Technocentre Régional de Montréal (TCR) se trouve sous la gouverne de la Régie Régionale de la Santé et des Services Sociaux de Montréal Centre. Ses employés proviennent de Syscor, société parapublique de services informatiques du Centre Hospitalier Universitaire (CHU) McGill. Le TCR a pour mandat :

- de gérer, selon le mandat reçu, les infrastructures technologiques mises en commun au niveau régional;
- d'assister, conseiller et supporter les établissements dans la mise en place et l'exploitation de leurs télécommunications sur le RTSS;
- d'offrir des services de partage d'infrastructures à sa clientèle, en occurrence les établissements du réseau;
- de favoriser l'autonomie des établissements par le transfert de connaissances, en complémentarité avec les besoins des établissements;
- d'assumer le leadership technologique auprès des établissements;
- de favoriser la concertation entre les établissements.

Le TCR offre à près de 147 établissements et à près de 400 points de service de la région de Montréal un ensemble d'applications et de services. Cela représente environs 25000 postes de travail. Parmi les applications et services offerts, se

retrouvent des bases de données relationnelles (Oracle), des applications de gestion de dossiers telles qu'intégration CLSC (iCLSC), des applications de partagiciel (Lotus Notes), un service de courrier électronique (Lotus Notes) ainsi que des accès sécuritaires à l'Internet et des accès sécurisés (VPN).

3.2 La sécurité

Comme nous le dit [Blobel, 2000], la mise en place d'une infrastructure sécuritaire est essentielle pour l'acceptation des technologies de l'information par les usagers du réseau de la santé. La protection des renseignements médicaux est un point particulièrement émotif pour ces bénéficiaires. Le projet européen AIM/SEISMED[3] [Smith, 1998] a identifié les principaux enjeux de la sécurité de l'information dans le secteur de la santé :

- l'identification de lignes directrices afin de maintenir un niveau de sécurité consistant dans l'ensemble des partenaires de la santé;
- la reconnaissance par les professionnels de la santé de l'importance de la sécurité de l'information, des impacts de l'absence de sécurité et de l'importance de considérer des mesures de protection adéquates;
- l'identification de preuves servant à démontrer le niveau de sécurité de l'information;
- la mise en place de standards pratiques et acceptés de tous qui permettront aux gestionnaires du secteur de la santé d'améliorer le niveau de sécurité de l'information.

[3] Advanced Informatics in Medecine / Secure Environment for Information Systems in Medicine.

Nos observations indiquent que ces enjeux sont assez près de ceux du TCR et fort probablement de l'ensemble des établissements du secteur de la santé au Québec.

Tel que décrit sur le site Internet du RTSS[4], plusieurs aspects de la sécurité de l'information ont été pris en compte dans le cadre de sa mise en oeuvre. En tant que fournisseur de l'infrastructure de télécommunication, le Groupe des Télécommunicateurs du Québec (GTQ) a pris en charge le réseau virtuel privé. Le réseau étendu privé RTSS est organisé en huit réseaux régionaux ségrégés par des pare-feu[5]. Il utilise un plan d'adresses IP privé communément appelé de classe 10[6].

Tous les autres aspects de la sécurité sont délégués aux acteurs du secteur sociosanitaire. L'orientation du MSSS à ce propos rend le secteur sociosanitaire autonome dans sa gestion de la sécurité [MSSS, 2003]. La mise en place de structures pour traiter des autres aspects de la sécurité est démarrée depuis peu.

3.3 Obligations légales

De façon générale, le serveur WebTCR comme l'ensemble des systèmes d'information du TCR sont soumis aux mêmes dispositions légales qui s'appliquent aux centres hospitaliers, CLSC, régies régionales, à la RAMQ et au MSSS. Ces dispositions légales sont un élément déterminant dans tout processus d'analyse des

---

[4] http://www.msss.gouv.qc.ca/rtss/main.html

[5] Système de protection placé entre un réseau local et un autre réseau (e.g. Internet). Cette barrière sert à assurer la sécurité des informations internes au réseau en filtrant les entrées et en contrôlant les sorties selon une procédure établie.

[6] Conformément aux assignations d'adresses de l'Internet Assigned Numbers Authority, les adresses dites de classe 10 consiste en un bloc d'adresses IP de 10.0.0.0 à 10.255.255.255 qui ne sont pas redirigé par les commutateurs et aiguilleurs du réseau InterNet.

menaces et des risques d'un système d'information dans le secteur de la santé au Québec. Décrites en détail dans les documents officiels de la Commission d'accès à l'information du Québec [Boudreau, 2001, nous identifions ici les principales lois qui trouvent une application :

- la Charte des droits et libertés de la personne (L.R.Q. chapitre C-12)
- la Charte canadienne des droits et libertés
- le Code civil du Québec
- la Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels (Loi sur l'accès, L.R.Q., chapitre A-2.1)
- la Loi sur les services de santé et les services sociaux (LSSSS, L.R.Q., chapitre S-4.2)
- la Loi sur la protection des renseignements personnels dans le secteur privé (Loi sur le secteur privé, L.R.Q., chapitre P-39.1)
- la Loi médicale, (L.R.Q., chapitre M-9)
- la Loi concernant le cadre juridique des technologies de l'information (L.Q., 2001, chapitre 32)
- le Code des professions (L.R.Q., chapitre C-26) et les lois professionnelles
- les codes de déontologie d'ordres professionnels oeuvrant dans le secteur de la santé

Comme le dit [Boudreau, 2001] :

> *Du serment d'Hippocrate à la LSSSS, la sensibilité des renseignements relatifs à la santé a toujours été largement reconnue et les règles de confidentialité ajustées en conséquence. […] Or, jusqu'à preuve du contraire, l'article 19 de la LSSSS trace clairement la conduite à suivre : les renseignements contenus dans le dossier d'un usager sont confidentiels et ils ne peuvent être communiqués qu'avec le consentement de cet usager ou si l'une des exceptions de la LSSSS trouve application.*

Bien qu'il soit clair que les renseignements nominatifs sont confidentiels (Loi sur l'accès, L.R.Q., chapitre A-2.1, Art. 53), le nom, le titre, la fonction, l'adresse et le numéro de téléphone du lieu de travail et la classification, y compris l'échelle de traitement rattachée à cette classification, d'un membre du personnel d'un organisme public sont des renseignements à caractère public. Cependant ces renseignements publics ne peuvent avoir pour effet de révéler le traitement d'un membre du personnel d'un organisme public (Loi sur l'accès, L.R.Q., chapitre A-2.1, Art. 57). Cette information est confidentielle.

4 Analyse des menaces et des risques

Nous avons effectué une analyse des menaces et des risques en utilisant la méthodologie que nous avions identifiée lors de la proposition de travail de synthèse. Nous avons débuté par des recherches bibliographiques, afin d'identifier quelles sont les méthodologies disponibles pour effectuer l'analyse des menaces et des risques. Nous avons choisi d'utiliser une méthodologie basée sur le 'Guide d'évaluation de la menace et des risques pour les technologies de l'information', rédigé et publié par la sous-direction de la sécurité des technologies de l'information de la Gendarmerie Royale du Canada. [GRC, 1994] Cette méthodologie qualitative a été choisie car elle correspondait aux objectifs de notre recherche. De plus, bien qu'il existe un grand nombre de méthodologies, celle-ci avait l'avantage d'être disponible sans frais et ne nécessitait pas l'achat d'une documentation coûteuse. Cependant nous avons effectué certaines modifications.

D'abord nous avons adapté la méthodologie afin qu'elle tienne compte des obligations légales du TCR. Puis, suite à nos rencontres initiales avec les gestionnaires du TCR, nous avons apporté un certain nombre d'éclaircissements aux différentes définitions et à l'ordonnancement des activités. Ensuite, dans la phase préparatoire identifiée sur la figure 3 (Analyse des menaces et des risques), nous avons effectué des recherches bibliographiques afin d'identifier les principaux enjeux de l'analyse des menaces et des risques dans les organisations en général et dans le secteur de la santé en particulier. Nous avons ensuite documenté la méthodologie d'analyse de risques et de menaces choisies dans un document à l'intention de l'organisation. Nous avons aussi préparé des tableaux tels que présentés dans ce document, afin de faciliter le travail. Nous avons aussi établi un plan de projet détaillé en utilisant le progiciel Microsoft Project. Une fois ce travail complété, nous avons rencontré les participants de l'organisation, afin de leur présenter la méthodologie et planifier l'exécution de l'analyse des menaces et des risques. Cette présentation s'est

faite lors de la réunion de lancement du projet qui avait été planifiée lors la proposition de travail de synthèse. Cette présentation a donné lieu à de nouveaux échanges sur le processus proposé. Les participants ont demandé des éclaircissements sur certains points de la méthodologie qui nous ont amené à modifier les documents afin de prendre en compte leurs commentaires. C'est aussi à cette étape que nous avons identifié les principaux participants de l'organisation aux différentes étapes du projet.

Nous avons identifié deux principaux groupes de participants. Le premier groupe est composé de gestionnaires de l'organisation. Ce groupe de participants dispose de connaissances approfondies des principaux objectifs d'affaires de l'organisation. De plus, il dispose d'une excellente compréhension des contraintes de l'organisation. C'est ce groupe qui participera à l'analyse des menaces et des risques. Le second groupe est composé de techniciens et de gestionnaires intermédiaires impliqués dans l'exploitation du système d'information analysé. Ce groupe participera à l'analyse des vulnérabilités, à l'exécution des tests et à l'analyse technique des résultats. Le groupe des gestionnaires participera aussi à l'analyse des résultats mais en les considérant en relation aux objectifs d'affaires de l'organisation.

La méthodologie d’analyse des menaces et des risques propose un processus qui se divise en trois étapes principales soit l'analyse d'un élément l'évaluation de la menace et l'évaluation des risques, tel que présenté dans la figure 3.

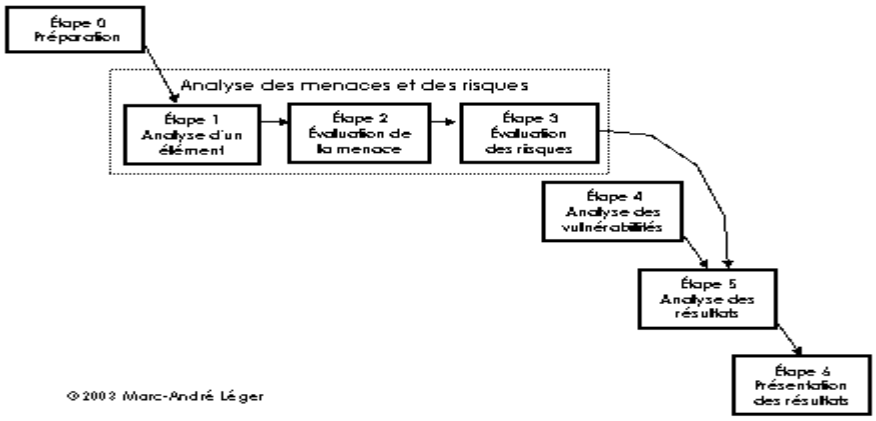

Figure 3 : analyse des menaces et des risques

L'analyse des menaces et des risques est précédée par une étape préparatoire (0). C'est à la suite de ces trois étapes de l'analyse des menaces et des risques (1, 2 et 3) que sera réalisée l'analyse des vulnérabilités identifiées sur le tableau par l'étape quatre (4). Ce chapitre décrit le processus employé et les résultats des étapes 0 à 3.

4.1 Analyse de l'élément

L'analyse de l'élément a été divisée en trois étapes. Premièrement nous avons identifié l'élément, son nom, sa fonction, ses composantes et sa configuration. En second lieu, nous avons identifié quels sont les individus qui en sont responsables. Finalement, nous avons rédigé un énoncé de sensibilité qui décrit et définit les besoins du système en matière de sécurité de l'information. L'ensemble de ces informations a été intégrée à un rapport d'étape. Pour la réalisation de cette analyse nous avons travaillé avec un groupe composé de gestionnaires du TCR. Ce groupe inclut les individus suivants :

- Gilles Blanchette ingénieur, Chef Développement et Déploiement, Secteur des Systèmes et des Technologies de l'Information, Régie Régionale de Montréal-Centre
- Jean-Pierre Cordeau, Ingénieur, M.Sc.A, Coordonnateur RTSS – Montréal,
- Pierre Desautels, Chef, support et opérations

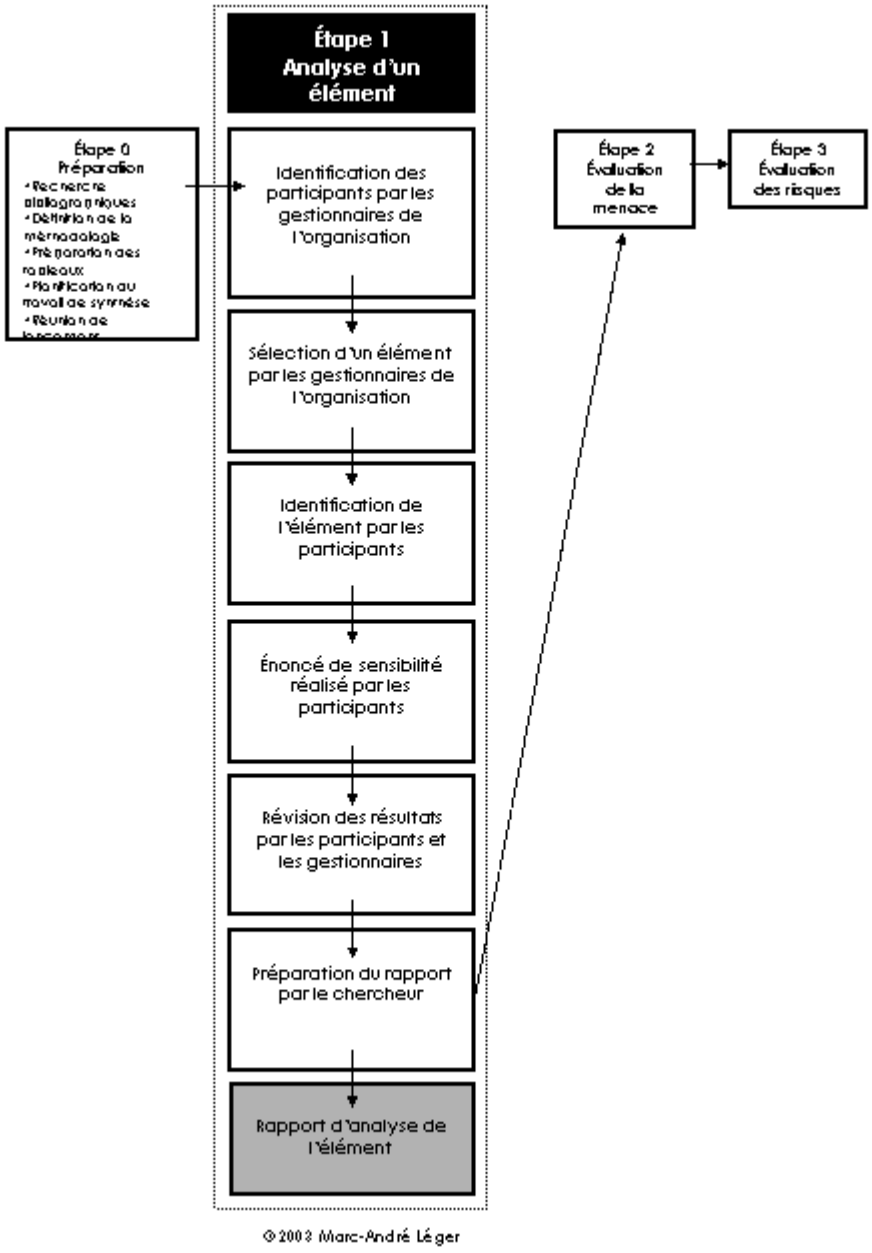

Figure 4 : analyse d'un élément

Nous avons transmis aux participants un document par courrier électronique. Ce document comprenait une description du processus d'analyse des menaces et de risques, tel que présenté précédemment et les tableaux qui allait être utilisés durant le

processus. Nous avons rencontré le groupe des gestionnaires dans les jours suivants. Lors de cette rencontre nous avons présenté au groupe de participants la méthodologie et avons recueilli leurs commentaires. Nous avons identifié certains éléments que les participants souhaitaient préciser. Nous avons par la suite modifié le document sur la méthodologie et le document remis précédemment afin de refléter ces changements. Nous avons alors transmis la version modifiée du document au groupe de gestionnaires par courrier électronique pour qu'ils puissent en prendre connaissance. À la rencontre suivante, quelques jours plus tard, nous avons procédé en complétant les tableaux selon la méthodologie transmise aux gestionnaires.

Le premier tableau complété fût le tableau 1, description de WebTCR. Nous avons complété le tableau en décrivant les éléments d'information, tel que présenté dans la section suivante. Ces informations ont par la suite été intégrées dans le document d'étape.

4.2 Identification de l'élément étudié

Item	Réponse identifié
Nom de l'élément :	WEBTCR
Description de l'élément étudié :	Serveur intranet principal pour utilisation interne du RTSS dans les régions de Montréal et de la Montérégie. IP : 10.128.36.99 Équipement : IBM x230 Intell PIII 1GHz, 2HD x 18GO, 896MB RAM OS: Red Hat Linux 7.3 Apps: Apache 1.3.23, Tomcat-Jakarta 4.1.18 Lien LDAP à Notes pour authentification Lien JDBC à un serveur MS-SQL (Win 2K)
Localisation :	TCR Local 135
Fonction principale :	• Serveur web principal pour utilisation interne du RTSS pour la région de Montréal; • Portail RH des régions de Montréal et de la Montérégie.
Catégorie principale:	Pièces d'équipements
Coût de remplacement :	$10 000 (estimé)
État de l'élément :	en production

Tableau 1 : description de WebTCR

4.2.1 Nom de l'élément étudié

Le nom communément donné à cet élément par l'organisation est WebTCR.

4.2.2 Description de l'élément étudié

Il s'agissait d'identifier les aspects techniques, périphériques et la configuration particulière de WebTCR. Nous avons identifié qu'il s'agissait d'un serveur intranet (http) principal pour utilisation interne du RTSS dans les régions de Montréal et de la Montérégie.

4.2.3 Localisation

La localisation est le lieu où l'élément se trouve habituellement, soit le local 135 au TCR.

4.2.4 Fonction principale

La fonction principale décrit quel est l'usage habituel et planifié du WebTCR. Nous avons identifié qu'il y avait deux usages principaux :

- serveur intranet principal pour utilisation interne (intranet) du RTSS pour la région de Montréal;
- portail RH des régions de Montréal et de la Montérégie.

Comme serveur intranet, le serveur offre aux utilisateurs des informations de nature générale et des informations de gestion sur l'utilisation du RTSS. Ces informations de gestion incluent des détails sur l'architecture du réseau RTSS, la configuration de router et des serveurs Lotus Notes, Oracle ainsi que le code source d'applications en utilisation dans le RTSS. À ces informations le TCR compte éventuellement ajouter des fonctionnalités à être définies dans le futur. Au sens de la Loi sur l'accès, ce système comporte des données à caractère public.

La portion portail RH du serveur WebTCR fonctionne comme serveur http (web). Il est réservé à l'usage des gestionnaires des régies régionales de la santé des régions de

Montréal-Centre et de la Montérégie. Le service de portail RH ne comprend pas d'informations nominatives et financières sur les employés des régies régionales, il comprend des informations sur des postes disponibles ou des appels de candidatures en cours. Au sens de la Loi sur l'accès, ce système comporte principalement des données à caractère public. Certaines des informations contenues sont à caractère confidentiel.

4.2.5 Catégorie

Détermine la catégorie dans laquelle se trouve l'élément étudié. Nous avons identifié qu'il s'agissait d'une pièce d'équipement.

4.2.6 État de l'élément

Il s'agissait de déterminer l'état actuel de l'élément. Nous avons déterminé que :

- le serveur WebTCR est un système d'information en développement;
- le portail RH des régions de Montréal et de la Montérégie est actuellement en production.

4.3 Identification des ayants cause

L'identification des ayants cause (stakeholder) a été effectuée en concertation avec les gestionnaires de l'organisation.

4.3.1 Gestionnaire responsable

Gilles Blanchette ingénieur, Chef Développement et Déploiement, Secteur des Systèmes et des Technologies de l'Information, Régie Régionale de Montréal-Centre a la responsabilité budgétaire de la gestion de WebTCR.

4.3.2 Personne ressource

Jean-Pierre Cordeau, Ingénieur, M.Sc.A, Coordonnateur RTSS – Montréal, Technocentre de Montréal a été identifié comme personne ressource. Cette personne est en mesure de fournir les informations sur la fonctionnalité de WebTCR, son contenu et sur son lien avec la mission de l'organisation.

4.3.3 Responsable technique

André Paradis, responsable support et opérations au TCR a la responsabilité de l'opération de l'exploitation et du support technique de WebTCR.

4.4 Énoncé de la sensibilité

L'énoncé de sensibilité a pour but d'évaluer l'élément étudié et son rôle dans l'organisation en vertu des besoins et obligations de l'organisation en relation aux sept principaux objectifs de la sécurité.

Tel que mentionné précédemment, le serveur WebTCR doit offrir un niveau de sécurité de l'information et des mesures de protection adéquates en fonction de ses obligations légales, particulièrement en relation avec la Loi sur l'accès et la LSSS. La Commission d'accès à l'information a fourni des lignes directrices et des recommandations à cet effet [CAI, 1992] [CAI, 2001] [CAI, 2002]. Dans l'énoncé de sensibilité, nous avons cherché à examiner le WebTCR en fonction des objectifs mentionnés ci haut. Les informations recueillies sur l'organisation, les obligations légales et les meilleures pratiques de l'industrie (Best Practices) mentionnées ont servi à élaborer l'énoncé de sensibilité. Afin d'assister, nous avons utilisé des questions sur les besoins en matière de sécurité de l'information, tel que proposé dans [GRC, 1994]. Nous avons enrichi les questions proposés par [GRC, 1994] pour correspondre aux sept objectifs que nous avons identifiés, tel que proposé dans la norme ISO/EIC 17799 :2000(E). La méthodologie d'analyse des menaces et des

risques de [GRC, 1994] se préoccupe des aspects de confidentialité, d'intégrité et de disponibilité alors que nous souhaitions travailler avec l'ensemble des sept objectifs mentionnés. Ces questions présentées dans les tableaux deux à huit (2 à 8) ont servi de point de départ aux discussions. Le chercheur a recueilli les commentaires des gestionnaires lors d'une rencontre de groupe. Ceux-ci ont été compilés et ces informations ont été intégrées dans l'énoncé de sensibilité. Ce document a été révisé avec le groupe des gestionnaires lors d'une rencontre subséquente. Finalement l'énoncé de sensibilité a été intégré au document d'analyse, qui constitue le livrable de l'étape 1 : Analyse de l'élément.

4.4.1 Niveau de confidentialité requis

La **confidentialité** identifie la sensibilité de l'information ou des biens à une divulgation non autorisée [GRC, 1994]. Elle est fréquemment évaluée à l'aide d'une cote de classification ou d'une désignation correspondant au niveau de dommage produit advenant une divulgation non autorisée. Dans certains cas, le degré de confidentialité peut varier en fonction du temps. Ainsi, certaines données peuvent devoir demeurer secrètes pendant qu'on les recueille et qu'on les traite, mais à partir du moment où celles-ci sont publiées et deviennent un document public, elles n'exigent plus le même degré de confidentialité. D'autres données, cependant, peuvent devenir plus confidentielles une fois regroupées. Afin d'évaluer les effets d'une perte de confidentialité, nous avons cherché à mettre en rapport le degré de sensibilité des données et les conséquences d'une divulgation inopportune. Bien que le système d'information WebTCR ne contienne pas de données cliniques, il contient des informations nécessaires au bon fonctionnement du réseau RTSS.

Lors de rencontres entre le chercheur principal et le groupe des gestionnaires, nous avons déterminé le niveau de confidentialité des données requis pour le serveur WebTCR. En nous référant aux objectifs de sécurité, à la culture de l'organisation, à la mission de l'organisation et en fonction de facteurs externes, comme les

obligations légales du TCR et les lignes directrices de la CAI, nous avons été en mesure de définir les attentes de l'organisation en matière de confidentialité vis-à-vis du système d'information WebTCR. Nous avons par la suite intégré es informations dans un tableau, tel que présenté dans le tableau 2.

la confidentialité des données	
Question	Réponse identifié
Quel est le niveau de confidentialité des données requis pour l'élément étudié ?	Le portail RH doit être disponible uniquement pour les gestionnaires des établissements des régions de Montréal et de la Montérégie. Le serveur Intranet devrait être accessible uniquement aux utilisateurs de la région Montréal-Centre qui y ont été autorisés.
Quelles sont les informations contenues par l'élément ?	Les informations à caractère public. Les documents internes à l'organisation. Les informations sur les comptes utilisateurs. Les informations sur les conventions collectives et les négociations de conventions collectives des employés du réseau de la santé. Les politiques et procédures en matière de gestion des ressources humaines. Les informations de nature confidentielle.
Quel est l'impact de la divulgation des informations contenues ?	Pertes économiques. Pertes de réputation.

Tableau 2 : confidentialité des données

4.4.1.1 Nature des informations contenues par l'élément

Il s'agissait de déterminer le type de données qui se trouvent dans WebTCR Sans effectuer un inventaire complet et détaillé, nous avons estimé à haut niveau les types de données. L'évaluation de la nature sensible de WebTCR a été effectuée en fonction des éléments de données qui sont le plus critique à la mission du MSSS et des organismes qui utilisent le RTSS et en fonction de facteurs externes, comme les obligations légales.

4.4.1.2 Impact de la divulgation des informations

L'organisation voudra déterminer quel serait l'impact de la divulgation des données. Elle devra se poser la question suivante : si les informations contenues dans l'élément étudié étaient divulguées, quel serait l'impact économique, commercial ou organisationnel estimé. Les praticiens du TCR ont indiqué qu'un des principaux impacts de la divulgation des informations contenues dans WebTCR serait lié à l'utilisation à mauvais escient des détails précis sur la configuration des différents éléments de l'infrastructure technique du RTSS. L'exploitation abusive de ces informations pourrait mener à des pertes économiques dus à des coûts de main-d'œuvre pour redresser un incident ou à des poursuites en dommages. En terme monétaire cet impact pourrait être estimé à entre $5 000 et dans des scénarios plutôt improbables quelques millions de dollars. Le principal impact serait la perte de réputation du personnel du TCR, ce qui est difficilement quantifiable.

4.4.2 Intégrité des données

L'**intégrité** est l'exactitude et l'intégralité des renseignements et des biens ainsi que l'authenticité des transactions [GRC, 1994]. L'intégrité se rapporte à l'exactitude et à l'intégralité des renseignements contenus dans le système et du système lui-même. Lorsque les exigences en matière d'intégrité sont élevées, comme c'est le cas pour les transactions financières dans les systèmes bancaires, les pertes financières possibles

fournissent une indication des sommes et des efforts qui doivent être investis dans les mesures de protection. Dans le secteur de la santé, les principaux handicaps à l'intégrité sont reliés au facteur humain qui intervient lors de la saisie et de l'utilisation des données [Barber, 1998]. Dans le cas de WebTCR, le chercheur principal et les participants ont déterminé que les besoins étaient moyens. C'est-à-dire que ce système d'information ne nécessite aucun contrôle particulier, au delà des mesures habituelles en place.

l'intégrité des données	
Question	Réponse identifié
Quel est le niveau d'intégrité des données requis pour l'élément étudié ?	Moyen
L'élément est-il sensible à l'altération accidentelle ou volontaire de son contenu :	Peu sensible
Quel est l'impact de l'altération des informations contenues ?	Perte de réputation Mineur

Tableau 3 : l'intégrité des données

4.4.2.1 Sensibilité à l'altération

Il s'agissait de déterminer si l'élément étudié est sensible à l'altération accidentelle ou volontaire de son contenu. Dans le cas de WebTCR, le chercheur principal et les participants ont déterminé que ce système d'information était peu sensible.

4.4.2.2 Impact de l'altération

Il s'agissait de déterminer quel serait l'impact de l'altération des informations contenues pour l'organisation. Dans le cas de WebTCR, le chercheur principal et les participants ont déterminé que l'impact était mineur. Le principal impact serait la perte de réputation du personnel du TCR, ce qui est difficilement quantifiable.

4.4.3 Disponibilité des données

La **disponibilité** est l'accessibilité d'un système d'information ou des données qu 'il contient, au moment opportun, pour exécuter certains processus [GRC, 1994]. Le système d'information, pour être considéré disponible, doit être en opération, utilisable aux fins voulues, au moment voulu. La disponibilité a trait à la continuité du service. Dans le cas de WebTCR, le chercheur principal et les participants ont déterminé que ce système d'information devait être disponible durant les heures normales d'ouverture des services administratifs des établissements de santé. Une période de maintenance préventive mensuelle a été adoptée.

la disponibilité des données	
Question	Réponse identifié
Quel sont les attentes de l'organisation pour l'élément étudié en matière de disponibilité des données ?	Durant les heures d'affaires. Une période de maintenance est prévue un jour ouvrable par mois, à tous les mois.
Quelle est la durée maximale acceptable de non-disponibilité, d'immobilisation ou de bris de cet élément ?	Huit (8) heures.

Tableau 4 : la disponibilité des données

4.4.3.1 Durée maximale acceptable de non disponibilité

Il s'agissait ici de déterminer la période de temps maximale que l'élément étudié peut être en condition de non disponibilité sans avoir de conséquences significatives pour l'organisation. Dans le cas de WebTCR nous avons déterminé qu'une non disponibilité de huit (8) heures était acceptable.

4.4.3.2 Non répudiation des transactions

La **non répudiation** ou l'**irrévocabilité** réfère à la permanence dans le temps et à la démontrabilité tangible de l'existence d'une transaction. La non répudiation des transactions nécessite que l'ensemble des individus ou des systèmes mènent à terme une transaction avec succès [Kalla, 1999]. Les systèmes d'information partie à la transaction doivent générer et conserver des preuves de la transaction, de sa source et de sa destination. [Kremer, 2002]. Dans les cas où la transaction a valeur de contrat entre les parties, un système de non répudiation des transactions pourra s'avérer utile [ISO/EIC17799 :2000(E)].

Il s'agissait d'identifier quels sont les besoins et quelles sont les mesures en place pour assurer la non répudiation des transactions. Dans le cas de WebTCR nous avons déterminé qu'il n'y avait aucun besoin particulier identifiable.

la non-répudiation des transactions	
Question	Réponse identifié
Quel sont les besoins en matière de non répudiation des transactions ?	Journalisation des transactions conformément aux directives de la CAI.
Quelles sont les mesures en place pour assurer la non répudiation des transactions ?	Journalisation sommaire de toutes transactions selon la configuration des serveurs.

Tableau 5 : la non répudiation des transactions

4.4.4 Authentification des utilisateurs

L'**authentification** des utilisateurs définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, l'identité d'un utilisateur d'un système d'information. Les trois catégories principales d'authentification d'un utilisateur sont :

- l'authentification d'une information connue de l'utilisateur légitime (e.g. un mot de passe);
- l'authentification d'un objet détenu par l'utilisateur légitime (e.g. une carte à puce);
- l'authentification d'une caractéristique distincte de l'utilisateur lui-même (e.g. biométrie, empreintes digitales).

Il s'agissait de déterminer les besoins pour WebTCR en matière d'authentification des utilisateurs selon les rôles et responsabilités qu'ils occupent dans l'organisation.

Nous avons déterminé que le niveau actuellement, une authentification à un facteur basé sur une information connue de l'utilisateur étaient suffisante.

l'authentification des utilisateurs	
Question	Réponse identifié
Quel sont les mesures en place en matière d'authentification des utilisateurs ?	□ un (1) facteur (userID + mot de passe) validé via LDAP sur le serveur Lotus Notes

Tableau 6 : l'authentification des utilisateurs

4.4.5 Authentification de l'origine des données

L'**authentification** de l'origine des données définit des mécanismes et des processus qui sont utilisés pour identifier, avec un niveau de certitude déterminé, la source d'une donnée stockés dans un système d'information. L'utilisation de journaux des transactions (log) est un des mécanismes utilisés pour permettre l'authentification de l'origine de données à posteriori.

Il s'agissait pour l'organisation de déterminer quels sont les besoins pour WebTCR en matière d'authentification de l'origine des données. Nous avons déterminé que le besoin en cette matière est que les données doivent provenir d'utilisateurs légitimes selon des règles d'affaires internes aux établissements, à la régie régionale ou au MSSS.

l'authentification de l'origine des données	
Question	Réponse identifié
Quel sont les besoins pour l'élément étudié en matière d'authentification de l'origine des données ?	Les données doivent provenir d'utilisateurs autorisés à utiliser le système selon des règles d'affaires internes aux établissements, à la régie régionale ou au MSSS.

Tableau 7 : l'authentification de l'origine des données

4.4.6 Contrôle des accès

Le **contrôle des accès** aux informations contenues dans un système d'information d'une organisation devrait être établi en fonction de ses objectifs et de ses obligations [ISO/EIC17799 :2000(E)]. Les systèmes de contrôle d'accès comprennent l'ensemble des mécanismes de vérification, de contrôle et de journalisation (log) de l'utilisation d'un système d'information ou des données qu'il contient.

Il s'agissait pour l'organisation de déterminer quels sont les besoins pour l'élément étudié en matière de contrôle des accès. Dans le cas de WebTCR, seuls les utilisateurs dûment autorisés doivent avoir accès aux divers éléments de données avec des droits établis selon un profil d'utilisateur. Nous retrouvons deux types de profils d'utilisateurs, soit un premier pour les utilisateurs ordinaires, le second pour les utilisateurs ayant des tâches d'administration ou de supervision du serveur.

le contrôle des accès	
Question	Réponse identifié
Quel sont les besoins pour l'élément étudié en matière de contrôle des accès ?	Seuls les utilisateurs dûment autorisés doivent avoir accès aux divers éléments de données avec des droits établis selon un profil d'utilisateur.

Tableau 8 : le contrôle des accès

4.4.7 Désignation en vertu d'une politique

Nous souhaitions ici déterminer les cotes de sécurité ou la désignation en vertu d'une politique de gestion documentaire de l'information contenue sur WebTCR. Cependant il n'y a pas de politique actuellement en place. Nous avons désigné l'information comme étant de nature confidentielle au sens de la Loi sur l'accès.

4.5 Évaluation de la menace et des risques

L'**évaluation des menaces et du risque** consiste à observer, dans un processus formel, la relation entre la menace et le risque pour en évaluer la probabilité [GRC, 1994]. À cette étape du travail de synthèse, nous souhaitions identifier les différentes menaces susceptibles d'affecter le serveur WebTCR, de les catégoriser, d'en évaluer la probabilité de réalisation, l'impact et de déterminer le niveau de risque pour l'organisation compte tenu de l'efficacité des mesures de protection existantes ou proposées. L'évaluation des menaces et des risques est nécessaire afin de déterminer les risques courus par l'organisation lorsque les mesures de protection existantes ou proposées sont jugées insuffisantes pour protéger l'élément étudié contre une menace donnée. L'évaluation des risques a été effectué de deux façons: d'abord à la lumière des mesures de protection en place en les inventoriant, puis en tenant compte des mesures de protection proposées. L'évaluation des menaces a d'abord nécessité l'identification des menaces. Nous avons ensuite évalué le risque associé à chaque menace identifié dans la typologie des menaces. Nous avons accompli cet objectif en complétant les tableaux d'analyse des menaces et des risques (tableau 13) pour chaque menace identifiée. La Figure 5 ci-contre, présente les principales étapes.

La réalisation de cette étape a nécessité la participation de praticiens du TCR :

- Gilles Blanchette ingénieur, Chef Développement et Déploiement, Secteur des Systèmes et des Technologies de l'Information, Régie Régionale de Montréal-Centre
- Jean-Pierre Cordeau, Ingénieur, M.Sc.A, Coordonnateur RTSS – Montréal,
- Pierre Desautels, Chef, support et opérations
- André Paradis, Responsable support et opérations.

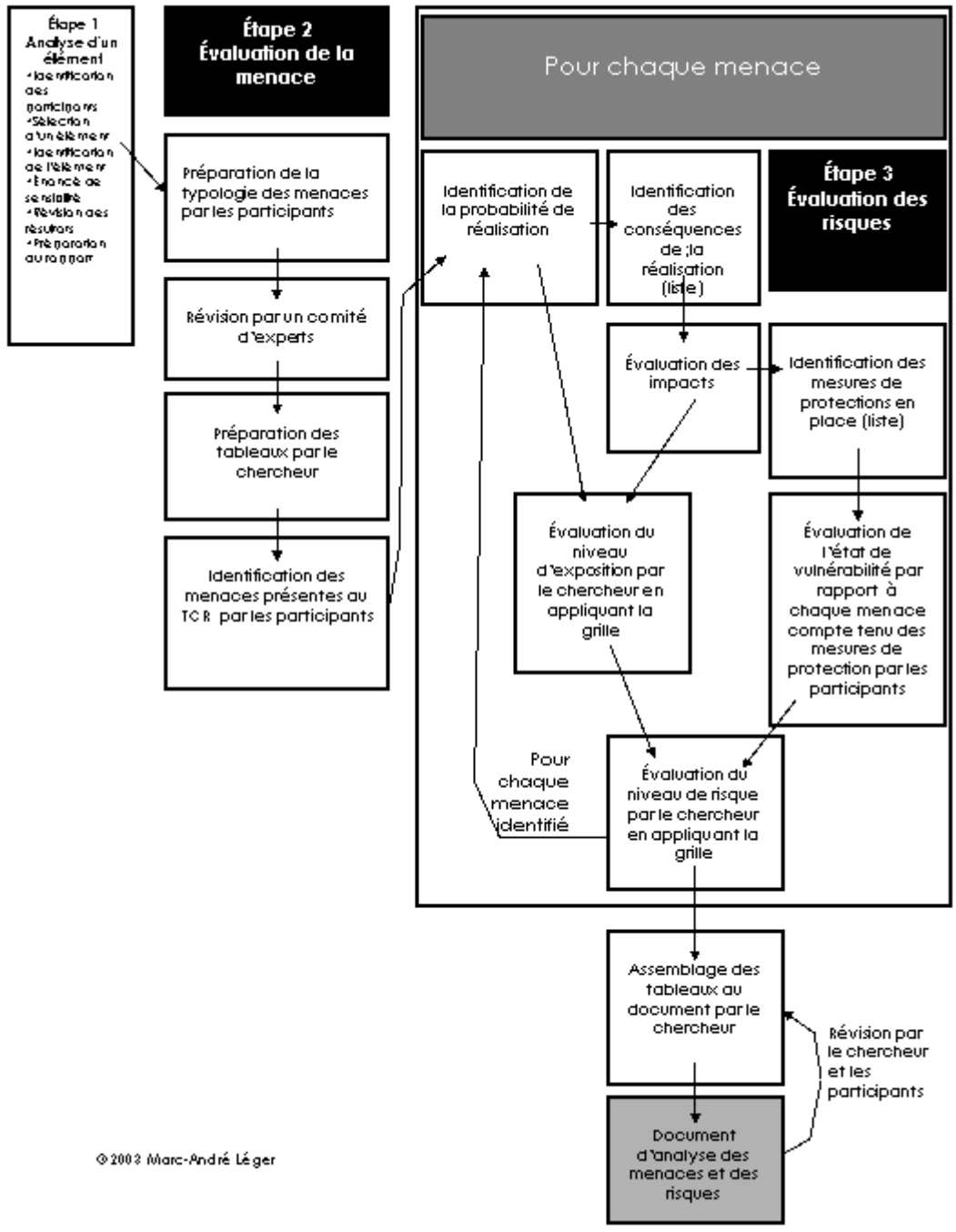

Figure 5 : évaluation de la menace

Le principal objectif de cette étape était d'identifier le niveau d'exposition à une menace pour WebTCR et les données qu'il contient.

4.5.1 Typologie des menaces

Nous avons cherché à identifier et à catégoriser les principales menaces à la sécurité de l'information du TCR, tel que défini par l'énoncé de sensibilité. Nous avons ensuite utilisé les réponses aux questions de la section précédente et la connaissance de l'organisation par les participants de l'organisation pour établir cette relation aux objectifs de la sécurité.

Nous avons débuté par effectuer des recherches afin d'identifier les différentes menaces. En effectuant des recherches sur Internet nous avons utilisé 'Argus 2000' comme point de départ. Avec ces informations nous avons construit une liste que nous avons enrichie avec des informations recueillies dans des articles récents sur la sécurité de l'information. Mentionnons entre autres [Denning, 2000], [Jordan, 1998], [Landwehr, 1981], [Maguire, 2002]. Nous avons ensuite catégorisé ces menaces et y avons ajouté de brèves descriptions sur le modèle proposé par 'Bierman 2002'. Puis nous avons communiqué cette liste par courrier électronique à un groupe de sept spécialistes des technologies de l'information au Canada, en France, au Danemark et aux États-Unis. Nous avons intégré leurs commentaires et les avons utilisés pour effectuer des précisions à notre liste de menaces. Par la suite nous avons soumis cette liste aux participants du TCR. Nous les avons rencontrés et avons recueilli leurs commentateurs sur ces menaces. Encore une fois, nous avons corrigé la liste pour tenir compte des commentaires de ces participants.

Les menaces ont été classées en deux catégories principales :

- les menaces pouvant causer des dommages matériels;
- les menaces causant des dommages immatériels.

4.5.2 Les dommages matériels

La catégorie des dommages matériels comprend les dommages matériels ou physiques aux divers éléments des systèmes d'information d'une organisation. Ces atteintes ne représentent qu'un faible pourcentage des sinistres informatiques. Les pertes associées à ces dommages sont évaluées en fonction de la valeur de remplacement [Maguire, 2002]. Dans le cas de WebTCR, le coût de remplacement de l'équipement, incluant les coûts reliés à la configuration et la mise en service, est estimé à 10 000 $.

Les praticiens du TCR ont identifié qu'il y a eu dans le passé des incidents dûs à des bris de tuyaux. L'édifice où est situé l'élément étudié est âgé.

4.5.2.1 Phénomènes accidentels

Les phénomènes accidentels identifient les évènements causés par l'environnement technique des systèmes d'information. Ceux-ci incluent des évènements naturels dont les conséquences sont aisément identifiables.

4.5.2.2 Vandalisme

Le vandalisme identifie des situations par lesquelles une ou plusieurs personnes détruisent sciemment ou subtilisent un système d'information [Denning, 2000] [Denning, 2000(1)].

4.5.3 Les dommages immatériels

La catégorie des dommages immatériels comprend les dommages associés aux données, programmes, logiciels contenus dans un système d'information. Il s'agit aussi d'atteintes à la confidentialité, l'intégrité et la disponibilité des systèmes d'information. Ces atteintes représentent le plus grand nombre des sinistres informatiques. Les pertes associées aux dommages immatériels sont difficiles à

évaluer. ‘Maguire 2002’ suggère l’utilisation de *«worst case scenario »* pour une telle évaluation.

En se basant sur les obligations légales du TCR, le principal impact de la divulgation d’information est économique. Comme nous le dit la Loi sur l’accès, à moins qu’il ne s’agisse d’un cas de force majeure, l'organisme public qui conserve un renseignement personnel est tenu de la réparation d’un préjudice résultant d'une atteinte illicite à un droit reconnu en vertu de la Loi sur l’accès. En outre, lorsque l'atteinte est intentionnelle ou résulte d'une faute lourde, le Loi sur l’accès prévoit des dommages punitifs d'au moins 200 $ (Loi sur l'accès, L.R.Q., chapitre A-2.1, Art. 167). La jurisprudence actuelle [Godbout, 2002] fixe le montant des dommages moraux à 1 000 $.

4.5.3.1 Erreur

L’erreur est l’acte involontaire d’un membre de l’organisation ou d’un utilisateur légitime d’un système d’information à la suite d’une mauvaise manipulation. Il en résulte des dommages immatériels comme la perte d’un fichier, la mauvaise exécution d’un programme ou l’exécution d’une commande destructrice. Ces phénomènes peuvent aboutir à des pertes très importantes.

4.5.3.2 La fraude

La fraude représente une partie importante des sinistres informatiques. Il s’agit le plus souvent de virements bancaires frauduleux ou du vol de fichiers contenant des numéros de cartes de crédits. Ces actes peuvent être l’œuvre d’un tiers mais sont souvent le fait de membres d’une organisation.

4.5.3.3 Cyber-crimes

Nous avons regroupé sous le nom de cyber-crimes, les fraudes informatiques réalisées par l'intermédiaire de systèmes d'information ou de réseaux de télécommunication tels que le réseau InterNet. C'est l'intrusion illégale d'un tiers à l'intérieur d'un système d'information, d'une base de données afin de les manipuler, les altérer ou d'en tirer profit.

4.5.4 Liste des menaces

Phénomènes accidentels
Bris accidentel
Panne accidentelle
Accident périphérique
Incendie
Inondation
Panne de courant
Survoltage
Champs électromagnétiques
Vandalisme
Vol
Incendie
Sabotage
Guerre
Activisme
Terrorisme
Erreur
Erreur de manipulation
Erreur dans l'entrée des données
Erreur de programmation
Erreur de configuration
Erreur de gestion de la capacité
Vulnérabilité technologique
Fraude
Erreur volontaire dans l'entrée des données
Erreur volontaire de programmation

Cyber-crimes
Écoute (Keylogging)
Écoute réseau (Sniffer)
Virus Vers Cheval de Troie
Attaque ciblée immédiate
Attaque ciblée retardée
Attaque ciblée distribuée
Prise de contrôle
Cyber-squattage
Cyber-activisme
Cyber-terrorisme

Tableau 9 : liste des menaces identifiées

4.5.5 Probabilité de réalisation de la menace

Une fois que nous avons identifié les menaces, nous avons compilé une liste, présenté dans le tableau 9. Nous avons ensuite utilisé le tableau d'évaluation des menaces et des risques qui a été réalisé à l'étape 0 : Préparation. Nous avons préparé un tableau par menace en utilisant le modèle ci-bas (tableau 10). Ce sont ces tableaux complétés (Annexe A) qui ont été utilisés comme outils de saisie des informations pour l'analyse des menaces et des risques.

<table>
<tr><th colspan="4">Menace</th></tr>
<tr><th rowspan="6">Type de menace</th><th>Probabilité de réalisation</th><th>Impact</th><th>Niveau d'exposition</th></tr>
<tr><td>□ sans objet</td><td>□ nul</td><td>□ nul</td></tr>
<tr><td>□ faible</td><td>□ moins grave</td><td>□ faible</td></tr>
<tr><td>□ moyenne</td><td>□ grave</td><td>□ moyen</td></tr>
<tr><td>□ élevée</td><td rowspan="2">□ très grave</td><td>□ élevé</td></tr>
<tr><td>□ inconnue</td><td>□ inconnu</td></tr>
<tr><th colspan="4">Risque</th></tr>
<tr><th colspan="2" rowspan="6">Mesure de protection existante</th><th>État de vulnérabilité</th><th>Niveau de risque</th></tr>
<tr><td>□ sécurité excessive</td><td>□ nul</td></tr>
<tr><td>□ équilibre</td><td>□ faible</td></tr>
<tr><td rowspan="3">□ vulnérabilité</td><td>□ moyen</td></tr>
<tr><td>□ élevé</td></tr>
<tr><td>□ inconnu</td></tr>
</table>

Tableau 10 : analyse des menaces et des risques

Pour chacune des menaces identifiées, en utilisant l'ensemble des tableaux décrits dans la section précédente, les praticiens et le chercheur principal ont déterminé, d'après l'expérience des praticiens, quelle était la probabilité de réalisation de chaque menace. L'évaluation de la probabilité s'est effectuée par une discussion sur la nature de la menace et sur l'expérience de l'organisation par rapport à cette menace. L'analyse d'incidents passés ou le fait que la menace se soit réalisée dans le passé

ainsi que l'analyse de mesures correctrices ont eu une place importante dans les discussions. Au besoin nous avons consulté d'autres sources telles que les bases de données de vulnérabilité[7], les sites Internet des manufacturiers et des éditeurs de logiciels[8].

Les niveaux de probabilité ont été définis en utilisant une échelle qualitative :

- nous avons employé la mention **sans objet** pour indiquer que la menace n'est pas présente au TCR.
- la mention **Faible** a été employée lorsqu'il a été établi qu'il n'y a aucun précédent et qu'il est peu probable que la menace ne se concrétise.
- la mention **Moyenne** a été employée lorsqu'il y a des précédents et que la menace est vraisemblable.
- la mention **Élevée** a été employée dans les cas ou il y a de nombreux précédents et où la menace est fort probable.

À titre d'exemple, si l'on considère la menace Virus, nous avons évalué sa probabilité de réalisation comme élevée. Nous avons justifié cette réponse par les éléments historiques (c'est arrivé dans le passé) et les perspectives du futur (ça va arriver encore). Comme autre exemple, considérons le cyber squattage. Nous l'avons évalué comme ayant une probabilité de réalisation faible car ce n'est jamais arrivé, même si c'est possible, quoique peu probable que ça se produise.

---

[7] http://www.securityfocus.com/bid , http://cve.mitre.org/

[8] http://www.apache.org/ , http://www.redhat.com/ , http://www.linuxsecurity.com/

4.5.6 Impact

L'impact est le résultat, l'effet ou la conséquence de la réalisation d'une menace. Ainsi c'est la gravité de la conséquence qui détermine l'impact. Afin d'évaluer les conséquences, nous avons d'abord proposé un mécanisme simple d'évaluation fondé sur l'évaluation du préjudice En dressant une liste des conséquences envisagées si la menace se réalise, nous les avons catégorisés. L'évaluation des conséquences nous a permis de déterminer l'impact de chacune des menaces pour l'organisation, eut égard aux coûts estimés et aux coût perçus liés à une perte de confidentialité, d'intégrité ou de disponibilité.

Une fois ce travail de réflexion en groupe effectué, nous avons analysé l'ensemble des conséquences et qualifié l'impact en utilisant les valeurs qualitatives suivantes :

- la mention **sans objet,** si l'impact n'est pas pertinent dans une situation donnée;
- **Faible** s'il n'y a que peu d'impact;
- **Moyenne** si l'impact est significatif;
- **Élevée** si l'impact est important.

Dans les discussions de groupe, nous avons cherché à évaluer l'impact de chaque menace qui pourrait se concrétiser en l'absence de mesures de protection. Cela a été possible en utilisant les connaissances du serveur et de son environnement détenues par les participants. Nous avons cherché à comprendre et décrire les activités de l'organisation dans laquelle évolue WebTCR. Nous avons envisagé les effets possibles sur le travail accompli, sur l'organisation elle-même et sur chacun de ses éléments qui comptent sur les renseignements ou les services offerts par WebTCR. L'objectif des discussions en groupe fût l'atteinte d'un consensus dans lequel le point

de vue des participants de l'organisation primait sur l'opinion des chercheurs. Le rôle du chercheur à cette étape était principalement celui de facilitateur.

4.5.7 Niveau d'exposition

Le niveau d'exposition à une menace est une fonction de la probabilité de réalisation et des impacts. Ainsi pour faciliter l'évaluation nous avons produit un tableau de référence (tableau 11) basé sur la relation entre l'impact et la probabilité en nous référant au modèle présenté dans la méthodologie [GRC, 1994].

Impact / **Probabilité**	**Sans objet**	**Faible**	**Moyen**	**Élevé**
Sans objet	Sans objet	Nul	Nul	Nul
Faible	Sans objet	Faible	Faible	Moyen
Moyen	Sans objet	Faible	Moyen	Élevé
Élevé	Sans objet	Moyen	Élevé	Élevé

Tableau 11 : évaluation du niveau d'exposition

Une fois que les informations sur la probabilité de réalisation et sur les impacts ont été obtenues dans les rencontres avec le groupe des gestionnaires, le chercheur a complété les tableaux d'analyse des menaces et des risques en appliquant le tableau ci-haut (tableau 11) à chacune des quarante-quatre (44) menaces identifiées. Ces résultats apparaissent dans le section Analyse de la menace des tableaux d'analyse des menaces et des risques, tel que présenté en Annexe A.

4.5.8 Évaluation des mesures de protection existantes

La prochaine étape du processus consistait à déterminer les mesures déjà en place pouvant contrer chacune des menaces identifiées lors de l'étape précédente. En évaluant la protection dont dispose le TCR pour se protéger des menaces que nous avons identifiées, nous avons cherché à déterminer s'il subsistait des points faibles. C'est par la relation entre la menace et les mesures de protection en place que nous avons estimé, de manière qualitative, l'état de vulnérabilité de l'organisation.

Nous avons constaté que le TCR dispose des mécanismes habituellement trouvés dans des environnements similaires tels les journaux d'évènements (log) et les systèmes d'authentification des utilisateurs (code d'utilisateur et mot de passe). Nous donnons ici une liste des principales mesures de protection en place :

- pare-feu *(firewall*);
- système de détection d'intrusion du TCN;
- connections sécurisés (SSL);
- copies de sauvegarde;
- système d'alarme;
- gardien de sécurité;
- contrôles d'accès.

4.5.9 État de vulnérabilité

En consultation avec le groupe des gestionnaires nous avons envisagé la possibilité que soient exploités un ou plusieurs points faibles existant sur le serveur WebTCR. Une attention particulière a été portée aux moments où le serveur est le plus

vulnérable, par exemple dans les points de service, durant les heures d'accès au public. Les principaux facteurs considérés sont identifiés ici :

- la probabilité qu'une menace se concrétise;
- les motifs possibles pour exploiter les points faibles;
- la valeur du bien vulnérable pour l'organisation et pour l'agent menaçant;
- l'effort requis pour exploiter les points faibles.

Une fois examinée la possibilité qu'un ou plusieurs points faibles existant soit exploités, nous avons examiné les mesures de protection existantes pour établir leur équilibre en relation à la menace.

Aux fins de notre analyse, nous avons retenu trois états possibles:

- l'état de **sécurité excessive,** lorsque le niveau de protection est trop élevé par rapport à la menace ;
- l'état d'**équilibre,** lorsque la protection est adéquate;
- l'état de **vulnérabilité**, si les mesures de protection sont jugées insuffisantes.

Nous avons ainsi complété ces informations dans chacun des tableaux d'analyse des menaces et des risques, tel que présenté en Annexe A.

4.5.10 Niveau de risque

Après avoir déterminé l'état de vulnérabilité, nous avons utilisé une grille d'évaluation (tableau 12) afin de déterminer le niveau de risque. Ce tableau (12) représente le niveau de risque comme une fonction de la relation entre le niveau d'exposition à une menace et l'état de vulnérabilité par rapport à cette même menace.

Ce tableau (12) est basé sur le modèle proposé par ‘GRC 1994’. Nous y avons cependant apporté certaines améliorations pour qu’il soit plus conforme à la perception des participants et des chercheurs.

État de vulnérabilité / **Niveau d’exposition**	**Sécurité excessive**	**Équilibré**	**Vulnérable**
Faible	Faible	Faible	Moyen
Moyen	Moyen	Moyen	Élevé
Élevé	Moyen	Élevé	Élevé

Tableau 12 : évaluation du niveau de risque

Voici les trois principaux niveaux de risque que nous identifions au sein de l'organisation:

- **Faible** si le niveau de risque est bas;
- **Moyen** si le niveau de risque est moyen;
- **Élevée** si le niveau de risque est important.

Nos recherches indiquent qu’il ne semble y avoir aucun avantage économique justifiable à évaluer des risques exceptionnels [Gordon, 2002]. Les risques qui sont extrêmement élevés devraient être traités comme une certitude. Les risques qui sont très petits ne peuvent qu’avoir une infime influence sur le niveau de risque total de l’organisation ne devraient pas être considérés. L’effort requis à les identifier et les qualifier justifie, tel que suggéré par ‘Gordon 2002’, qu’ils soient omis. Ainsi dans ce

travail de synthèse nous n'avons pas considéré les menaces qui ont été identifiées comme certaines (identifiées comme tel dans le tableau 14 : sommaire du risque).

<table>
<tr><th colspan="5">Menace</th></tr>
<tr><th>Type de menace</th><th>Probabilité de réalisation</th><th>Impact</th><th>Niveau d'exposition</th><th></th></tr>
<tr><td rowspan="6">Accident périphérique</td><td>□ Sans objet</td><td>□ Nul</td><td>□ Nul</td><td></td></tr>
<tr><td>X Faible</td><td>□ Moins grave</td><td>□ Faible</td><td></td></tr>
<tr><td>□ Moyenne</td><td>X Grave</td><td>X Moyen</td><td></td></tr>
<tr><td rowspan="2">□ Élevée
□ Inconnue</td><td rowspan="2">□ Très grave</td><td>□ Élevé</td><td></td></tr>
<tr><td>□ Inconnu</td><td></td></tr>
<tr><th colspan="5">Risque</th></tr>
<tr><th colspan="2">Mesures de protection existantes</th><th>État de vulnérabilité</th><th>Niveau de risque</th><th></th></tr>
<tr><td colspan="2" rowspan="5">Copies de sauvegardes;
Possibilité de site de reprise dans une région périphérique</td><td>□ Sécurité excessive</td><td>□ Nul</td><td></td></tr>
<tr><td>□ Équilibre</td><td>□ Faible</td><td></td></tr>
<tr><td rowspan="3">X Vulnérabilité</td><td>□ Moyen</td><td></td></tr>
<tr><td>X Élevée</td><td></td></tr>
<tr><td>□ Inconnu</td><td></td></tr>
</table>

Tableau 13 : tableau d'analyse des menaces et des risques complété.

Nous avons ainsi complété les tableaux d'analyse des menaces et des risques (un tableau par menaces), tel qu'illustré dans le tableau 13. Nous avons complété l'ensemble des tableaux qui sont présentés en Annexe A.

Nous pouvons observer dans le tableau 13 que la probabilité de réalisation de la menace 'Accident périphérique' est considérée faible. Comme l'impact est considéré

comme grave, l'emploi de la grille d'évaluation du niveau d'exposition nous propose un niveau moyen. Après avoir identifié, en collaboration avec les participants de l'organisation, les mesures de protection en place, nous avons établi l'état de vulnérabilité. En appliquant la grille d'évaluation du niveau de risque, nous identifions que le niveau de risque pour cette menace est élevé.

Nous avons répété ce processus pour l'ensemble des quarante-quatre (44) tableaux d'analyse des menaces et des risques. Ce travail a été complété pour toutes les menaces par le chercheur principal dans un document présenté en Annexe A. Ce document a été envoyé au groupe des gestionnaires par courrier électronique pour consultation. Quelques jours plus tard le groupe des gestionnaires a été rencontré afin de valider les résultats et, au besoin, compléter certaines informations. Suite à cette rencontre un certain nombre de corrections ont été faites. Les résultats ont été soumis de nouveau aux praticiens par courrier électronique pour l'obtention d'un consensus. Quelques échanges ont été nécessaires, lorsqu'il y avait des différences d'opinions et la priorité a été accordée au point de vue des gestionnaires de l'organisation. Par la suite un tableau sommaire des résultats a été préparé. Les tableaux 13 et 14 présentent le sommaire des résultats de l'analyse des menaces et des risques.

Phénomènes accidentels	
Menace	**Niveau de risque évalué**
Bris accidentel	Certain
Panne accidentelle	Certain
Accident périphérique	Moyen
Incendie	Moyen
Inondation	Moyen
Panne de courant	Certain
Survoltage	Faible
Champs électromagnétiques	Faible
Vandalisme	
Vol	Faible
Incendie	Faible
Sabotage	Faible
Guerre	Faible
Activisme	Faible
Terrorisme	Faible

Tableau 14 : sommaire du risque

Erreur	
Menace	**Niveau de risque évalué**
Erreur de manipulation	Moyen
Erreur dans l'entrée des données	Faible
Erreur de programmation	Moyen
Erreur de configuration	Moyen
Erreur de gestion de la capacité	Faible
Vulnérabilité technologique	Moyen
Fraude	
Erreur volontaire dans l'entrée des données	Faible
Erreur volontaire de programmation	Faible
Cyber-crimes	
Écoute (Keylogging)	Faible
Écoute réseau (Sniffer)	Faible
Virus Vers Cheval de Troie	Moyen
Attaque ciblée immédiate	Moyen
Attaque ciblée retardée	Moyen
Attaque ciblée distribuée	Moyen
Prise de contrôle	Faible
Cyber-squattage	Faible
Cyber-activisme	Faible
Cyber-terrorisme	Moyen

Tableau 15 : sommaire du risque (suite)

5 Analyse des vulnérabilités technologiques

Une fois l'analyse des menaces et des risques du serveur WebTCR complétée (Étape 1 à 3 de la figure 1), la phase suivante de notre projet consistait à effectuer l'analyse des vulnérabilités technologiques (étape 4). La réalisation de l'analyse des vulnérabilités est essentiellement divisée en deux parties : l'exécution de l'analyse de vulnérabilités (étape 4) et l'analyse des résultats (étape 5), tel que présenté sommairement dans la figure 1 et de façon plus détaillée dans la figure 6 (page 67).

Dans un premier temps, dans un environnement de laboratoire, nous avons procédé à l'installation de LINUX sur un poste de travail en notre possession. Nous y avons installé le logiciel NESSUS que nous avons configuré et utilisé. Nous disposions à cette fin d'un laboratoire muni d'un analyseur de protocoles réseau et de différents postes de travail de type Windows. Nous avons effectué une dizaine de tests d'analyse de vulnérabilités dans cet environnement contrôlé. En effectuant différent tests, nous avons été capables d'affiner la configuration de LINUX et de NESSUS. Nous avons aussi été en mesure de développer une certaine expertise avec le logiciel.

En observant les résultats sur l'analyseur de protocole nous avons pu voir qu'il y avait peu ou pas d'impact sur les performances de réseaux à utiliser NESSUS pour l'analyse de vulnérabilités. Une fois ces tests effectués, nous avons planifié une rencontre avec André Paradis (Responsable, support et opérations) afin d'effectuer des test dans le laboratoire du TCR. En effet le TCR dispose d'installations de test dans ces locaux de la rue Saint-Joseph. C'est ainsi que lors de ces tests nous avons pu observer que les résultats de l'analyse de vulnérabilités semblaient incomplets. Nous avons ainsi interrompu les tests et cherché à comprendre la situation. C'est alors que nous avons découvert qu'une nouvelle version de NESSUS était disponible. Nous sommes retournés à notre laboratoire pour procéder à la mise à niveau et effectuer des tests additionnels pour retourner au laboratoire du TCR quelques jours plus tard. Une fois les tests effectués à la satisfaction des participants, la décision a été prise par

Jean-Pierre Cordeau (Coordonnateur RTSS – Montréal) d'autoriser les tests dans l'environnement de production.

Nous avons convenu du moment où seraient effectués les tests. Au moment déterminé nous avons procédé avec Dino Lolli (Technicien, support et opérations) à la mise en place de l'outil d'analyse des vulnérabilités Nessus sur le réseau de production et avons effectué les tests prévus. Nous avons débuté par un balayage de vulnérabilités sur un équipement bien identifié, le serveur Intranet WebTCR. Ce serveur est sur une plate-forme Linux / Apache tel que décrit précédemment lors de l'étape 1 (Analyse de l'élément).

Nous présentons dans ce chapitre les principales informations sur la mise en place et l'utilisation du logiciel NESSUS ainsi que les principaux résultats obtenus. Les principales activités sont identifiées sur la Figure 6.

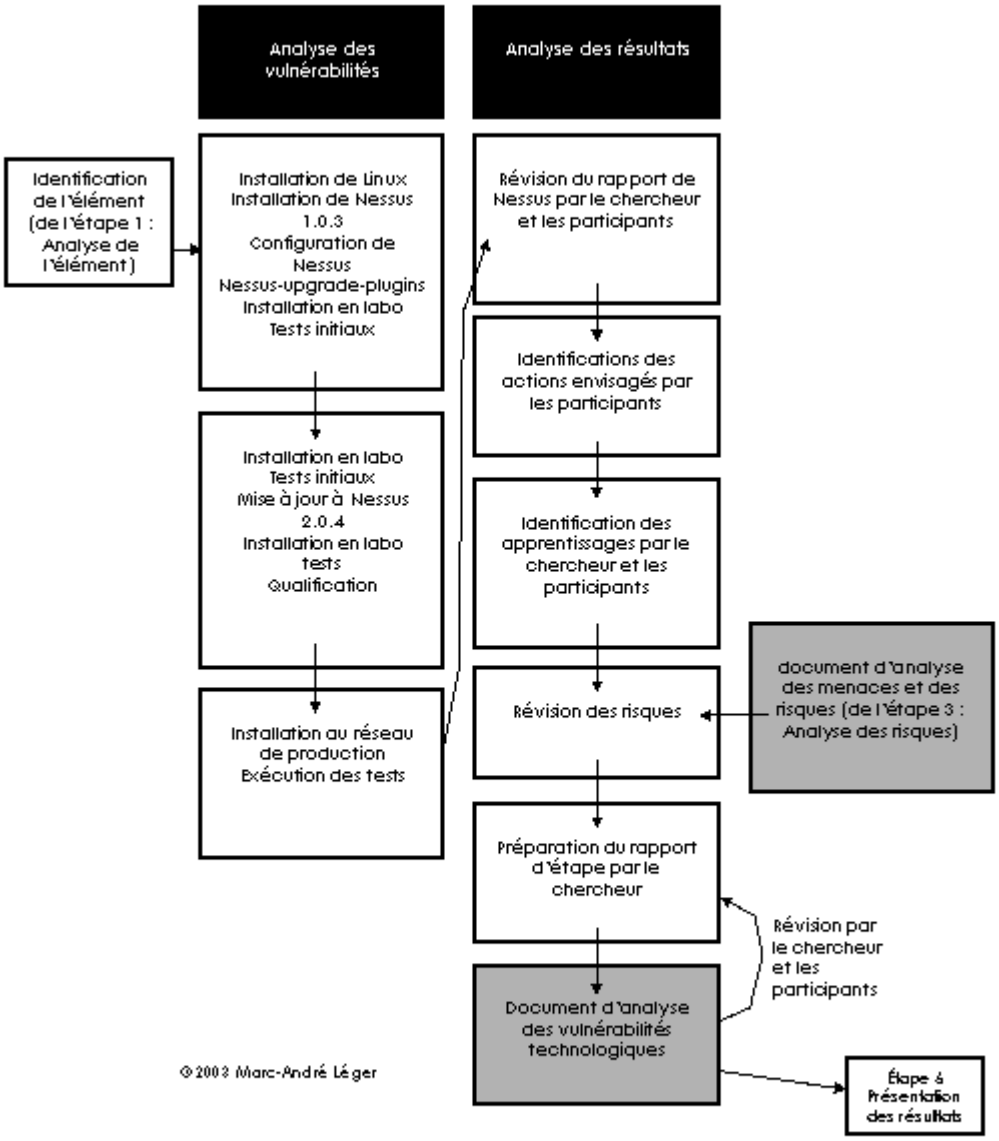

Figure 6 : analyse de vulnérabilités

5.1 Nessus

Nessus est un détecteur de vulnérabilités, développé par Renaud Deraison, disponible sous une licence de type Open source[9]. Ce logiciel permet d'effectuer un balayage réseau pour identifier des vulnérabilités en relation avec une base de signatures, un peu comme un progiciel anti-virus. L'identification de vulnérabilités par Nessus est directement attribuable à la présence d'une signature correspondante dans la base de données du logiciel.

Nessus fonctionne en mode client-serveur. Le serveur fonctionne dans l'environnement Linux, tandis que le client fonctionne sur divers systèmes d'exploitation, dont Windows. Puisqu'il s'agit d'un logiciel 'Open Source', les mises à jour du logiciel et des bases de données qu'il contient sont soumis à de nombreux facteurs externes qui sont particuliers à ce type de logiciels. L'analyse des vulnérabilités par Nessus est limitée par les signatures disponibles et installées. Il utilise des simulations de séquences d'instructions qui reproduisent les actions nécessaires pour identifier la présence d'une vulnérabilité. Dans cette section, nous discutons de la mise en place et l'utilisation du client et du serveur sur Linux, tel qu'il fut utilisé pour nos tests.

5.1.1 Installation

Nous avons choisi d'utiliser le système d'exploitation Debian/Linux version 3.0r1. Ce système d'exploitation peut être obtenu sous une licence 'Open source' depuis le site Internet http://www.debian.org . Nous n'irons pas dans le détail de l'installation de

[9] http://www.opensource.org/

Linux, il y a de nombreuses sources d'information à ce sujet[10]. Nous avons installé l'interface utilisateur Xwindows. Nessus a été installé en utilisant l'interface Gnome-APT. Cette installation a nécessité quelques essais et erreurs, le temps de trouver la configuration qui fonctionnait le mieux avec l'équipement disponible. Une fois la configuration finale déterminé, l'installation a nécessité quatre heures.

Nous estimons le coût total de la solution à :

Micro-ordinateur PIII-800	800.00$
Linux et Nessus	0.00$
Installation et configuration (4 heures x 50$)	200.00
Total :	1000.00$

Tableau 16 : coût de la solution utilisé

5.1.2 Plugins

Les *plugins* sont des modules de NESSUS. Ils contiennent un ensemble d'instructions et de scripts qui permettent d'effectuer un grand nombre de tests afin d'identifier des vulnérabilités technologiques. Les scripts de NESSUS sont écrits dans un langage appelé NASL[11]. En utilisant la commande *nessus-update-plugins* nous avons procédé à une mise à jour des plugins. Après la mise à jour le système comprenait 1541 plugins.

---

[10] Mentionnons particulièrement le Linux Documentation Project http://www.tldp.org/

[11] Nessus Attack Scripting Language

5.1.3 Limites de l'outil

Nous croyons qu'il est important de mentionner les limites du logiciel. Puisqu'il fonctionne en identifiant les vulnérabilités technologiques via le port réseau du serveur analysé, il ne peut identifier que les menaces qui sont 'visibles' de ce point de vue. Certain types d'attaques qui nécessitent l'accès au clavier de l'ordinateur ou au lecteur de disquettes, par exemple, ne peuvent pas être testés avec un outil comme Nessus. De plus, comme il utilise des plugins, à moins d'en créer, il n'est possible d'identifier que celles pour lesquelles des signatures sont disponibles.

5.2 Description des tests

En utilisant la plate-forme de gestion de réseau et le logiciel NESSUS, tel que décrit précédemment, il a été possible d'effectuer un certain nombre de tests en fonction des 1541 *plugins* installés sur les équipements ciblés. La durée de ces tests fut d'approximativement deux heures.

L'extrant détaillé de cette étape est un rapport des vulnérabilités disponible en Annexe B. Nous en reproduisons ici le rapport sommaire de NESSUS (Tableau 17) :

Service (port TCP/IP)	**Résultat identifié par NESSUS**
telnet (23/tcp)	Security warning(s) found
ftp (21/tcp)	Security notes found
www (80/tcp)	Security hole found
sunrpc (111/tcp)	Security notes found
inconnu (4600/tcp)	Security notes found
inconnu (4602/tcp)	Security notes found
inconnu (4601/tcp)	Security notes found

inconnu (4604/tcp)	Security notes found
inconnu (4603/tcp)	Security notes found
inconnu (4622/tcp)	Security notes found
inconnu (4621/tcp)	Security notes found
inconnu (4620/tcp)	Security notes found
inconnu (4619/tcp)	Security notes found
inconnu (4618/tcp)	Security notes found
inconnu (4617/tcp)	Security notes found
inconnu (4616/tcp)	Security notes found
inconnu (4615/tcp)	Security notes found
inconnu (4614/tcp)	Security notes found
inconnu (4613/tcp)	Security notes found
inconnu (4612/tcp)	Security notes found
inconnu (4611/tcp)	Security notes found
inconnu (4610/tcp)	Security notes found
inconnu (4609/tcp)	Security notes found
inconnu (4608/tcp)	Security notes found
inconnu (4607/tcp)	Security notes found
inconnu (4606/tcp)	Security notes found
inconnu (4605/tcp)	Security notes found
inconnu (4625/tcp)	Security notes found
inconnu (4624/tcp)	Security notes found
inconnu (4623/tcp)	Security notes found

ajp13 (8009/tcp)	No Information
zeus-admin (9090/tcp)	Security notes found
general/icmp	Security warning(s) found
general/tcp	Security notes found
sunrpc (111/udp)	Security notes found
ntp (123/udp)	Security warning(s) found
general/udp	Security notes found

Tableau 17 : rapport de Nessus

5.3 Résultats

Les résultats bruts des tests (Annexe B) en format texte (TXT) ont été envoyés par courrier électronique comme pièce jointe au chercheur principal. Ces résultats on été incorporés par le chercheur dans un rapport avec les résultats de l'analyse des menaces et des risques. Une colonne supplémentaire a été ajoutée au tableau détaillé du rapport de NESSUS afin de recueillir les commentaires des participants, tel que présenté au tableau 18. Le rapport produit contenait la liste des vulnérabilités technologiques, les impacts connus de l'exploitation de ces vulnérabilités et des pistes de solutions ou des actions possibles pour réduire les impacts. Ce rapport a été transmis par courrier électronique à tous les participants. Puis une rencontre a eu lieu pour analyser les résultats.

5.4 Analyse des résultats

Lors d'une rencontre, les praticiens et le chercheur principal ont procédé à analyser le rapport de NESSUS (Annexe B). Chaque vulnérabilité technologique identifiée par NESSUS a été analysée. Une discussion sur l'impact de chacune d'elles a eu lieu. L'impact des données recueilli par Nessus sur l'évaluation des menaces et des risques

avait été réalisé précédemment. En référence à sa compréhension du rapport de Nessus, Jean-Pierre Cordeau a apporté le commentaire suivant qui reflète bien l'opinion des participants de l'organisation:

> *'C'est intéressant, mais ça reflète une toute petite partie de la problématique de la sécurité de l'information'*

Selon lui, il serait plus utile d'attaquer un système d'information avec l'ensemble des systèmes reliés à celui-ci. Un système comme WebTCR utilise des bases de données situées sur d'autres serveurs ainsi que des liens avec les serveurs Lotus Notes. Les vulnérabilités de ces systèmes doivent être considérées en relation aux vulnérabilités et au système étudié. Bien que cette vision soit partagée par le chercheur principal, nous croyons cependant que le niveau de complexité accru et l'augmentation de la durée d'un processus couvrant un ensemble d'actifs doivent être considérés dans la détermination de l'envergure accordée à un processus d'analyse. Nous présentons, dans le tableau 18, le sommaire des observations recueillies lors de cette discussion et les actions envisagées pour réduire le niveau de risque.

Vulnérabilité technologique	Commentaire(s) des praticiens	Action envisagée
telnet (23/tcp)	Ce service est filtré de l'Internet au niveau du TCN; Il est accessible seulement depuis le TCR	• modifier les fichiers de configuration pour limiter les adresses IP ayant un accès ; • considérer la mise en place de OpenSSH
ftp (21/tcp)	L'accès FTP est nécessaire pour les mises à jour de pages sur le serveur Apache	• configurer des filtres (TCP Wrapper) afin de limiter les accès ; • remplacer FTP par un service OpenSSH
www (80/tcp)	Le problème associé au module mod_jk n'est pas une surprise; le module mod_jk fait le lien entre Apache et Jakarta ; des changements au module PHP serait difficiles à faire ; le développement en PHP est fait par une firme de consultants externes ; l'affichage de la version de Apache est volontaire afin de publiciser son usage par le TCR dans un but essentiellement pédagogique.	• mettre à jour le module mod_jk ;
sunrpc (111/tcp)	Ce service n'a pas d'utilité pour ce système.	• Il est proposé d'enlever ce service
4600/tcp à 4625/tcp	Ce service est inconnu; Il s'agit possiblement des ports utilisés pour les branchements aux bases de données;	• faire des recherches pour tenter d'identifier avec plus de certitude ce dont il s'agit ; • L'utilisation de TCP Wrapper pourrait sécuriser ce port
ajp13 (8009/tcp)	Ce service est utilisé par le module Tomcat	• Ce service est nécessaire
zeus-admin (9090/tcp)	Il s'agit du service d'indexation web	• Ce service est nécessaire

Tableau 18 : analyse du rapport de Nessus

Le consensus résultant des discussions est que, dans le cas de WebTCR, les vulnérabilités technologiques identifiées confirment le niveau de risque qui avait été déterminé lors de l'analyse des menaces est des risques. De manière plus précise, nous avons évalué moyen le niveau de risques en relation aux menaces de la catégorie 'Vulnérabilités technologiques'. Ainsi l'analyse des menaces et du risque ne nécessite pas d'être révisée par rapport au niveau de risque identifié précédemment au tableau de l'annexe A.

Lors de cette rencontre nous avons comparé les données recueillies aux meilleures pratiques de l'industrie (*best practice*), à la norme ISO/EIC 17799 :2000(E) ainsi qu'aux recommandations de la Commission d'accès à l'information du Québec, afin de proposer des processus refondus et d'identifier si certains éléments mériteraient d'être examinés avec plus de détails.

5.5 Présentation des résultats

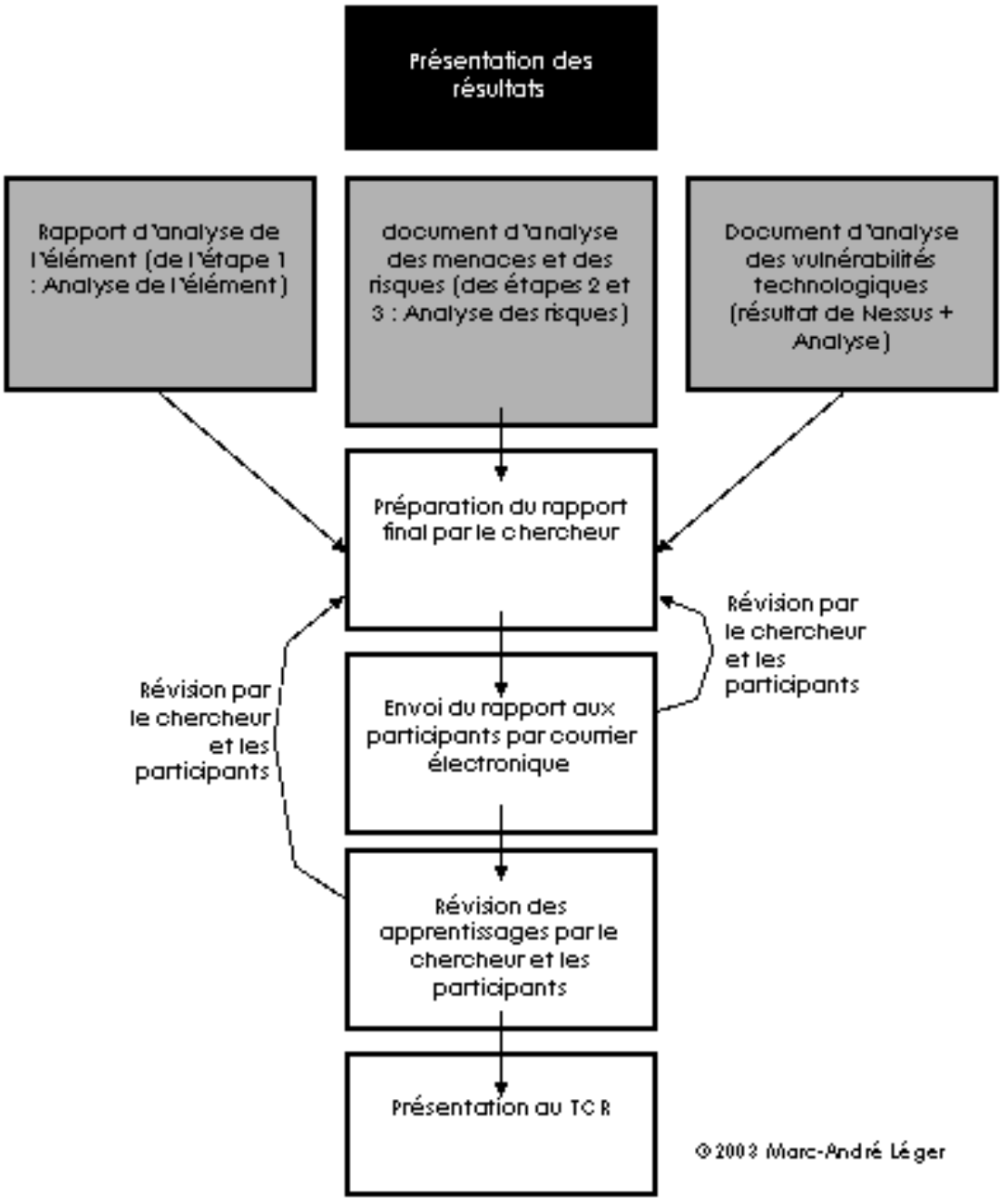

Figure 7 : présentation des résultats

Une fois l'analyse des vulnérabilités et l'analyse des résultats effectuées, nous avons assemblé les informations dans un rapport qui a été acheminé par courrier électronique aux participants, tel que présenté dans la figure 7. Les participants ont été rencontrés une semaine plus tard. Nous avons procédé à valider le rapport avec les participants, puis avons documenté l'ensemble des apprentissages du travail de synthèse pour leur utilisation dans le rapport final du travail de synthèse. Ces apprentissages sont présentés dans le chapitre suivant. C'est ainsi que nous avons produit le rapport final du point de vue de l'organisation, soit le rapport d'analyse des vulnérabilités et le rapport d'analyse des menaces et des risques. Du point de vue des participants de l'organisation c'est ce document qui aura le plus d'importance. Nous avons ensuite été en mesure de présenter les résultats à l'organisation et conclure l'analyse des vulnérabilités. Suite à la présentation des résultats aux participants et aux gestionnaires de l'organisation, nous avons été en mesure de procéder avec la prochaine étape de la méthodologie, l'identification des connaissances, présenté au chapitre suivant.

6 Identification des connaissances

La phase d'identification des connaissances est la phase finale de la méthodologie de recherche-action. Cette phase vise à identifier les succès et les échecs. Une fois toutes les étapes de l'analyse des menaces et des risques et l'analyse des vulnérabilités complétées, nous avons rencontré les participants afin de passer en revue les apprentissages du travail de synthèse. Ces éléments ont été compilés par le chercheur principal en collaboration avec le groupe des gestionnaires et le groupe des participants dans un rapport d'étape. Les leçons acquises ont été documentées et des modifications au cadre théorique et méthodologique ont été identifiés pour une recherche future. À cette fin deux rencontres ont été effectuées avec les participants mentionnés. La première rencontre a pris la forme d'un échange informel d'une durée de deux heures. Puis les informations recueillies par le chercheur ont été documentées et un rapport a été transmis aux participants par courrier électronique. Les participants ont suggéré des changements qui ont été intégrés au document. Ces informations ont été intégrées à un rapport sur l'ensemble du projet, qui a été soumis aux participants et discuté lors de la rencontre finale du projet avant la présentation officielle qui avait été prévue pour conclure le travail de synthèse. Ce chapitre contient le sommaire des principales leçons du travail de synthèse.

6.1 Leçons apprises

L'exécution du travail de synthèse avec la méthodologie choisie demande une participation active du chercheur principal et des participants. Dans le cadre de ce travail de synthèse il fut difficile de procéder au rythme envisagé lors de la proposition initiale. Le principal obstacle fut la difficulté à trouver des créneaux horaires disponibles de tous les participants impliqués. Bien qu'il fut possible de compenser par l'utilisation du courrier électronique, le volume d'informations que chaque participant devait consulter afin d'arriver à des consensus sur les différentes

étapes a rendu la tâche ardue aux participants. Ces praticiens ont des responsabilités opérationnelles qui peuvent rendre plus complexe la gestion de leur disponibilité.

Au cours de la réalisation du premier cycle de recherche, il est apparu que la pertinence des apprentissages du travail de synthèse est très significative pour l'organisation. Le TCR n'ayant pas de processus formel d'analyse des menaces et des risques ni de processus d'analyse des vulnérabilités, il apparaît que l'amélioration du niveau de la sécurité de l'information procurée par une analyse des menaces et des risques à elle seule est très significative. Relativement, l'amélioration du niveau de la sécurité de l'information procurée par un processus d'analyse des vulnérabilités est moins significative. Ainsi il semble nécessaire d'évaluer la pertinence des deux éléments d'analyse du risque et des vulnérabilités ensemble comme catalyseur pour l'amélioration de la position de l'organisation.

Pour bien mesurer l'impact de l'analyse des vulnérabilités, il aurait été préférable de procéder au travail de synthèse dans une organisation ayant déjà en place un processus formel de gestion du risque en matière de sécurité de l'information. Dans le cas présent le nombre de variables présentes, l'importance relative d'une de celles-ci et la méthodologie choisie dans la recherche a pour effet de diminuer le niveau de certitude des résultats obtenus. Nous croyons que la précision des résultats de notre travail de synthèse est affectée par le nombre de variables. Pour obtenir des données plus fiables, avec la méthodologie proposée, nous aurions mieux fait d'effectuer un travail de synthèse dans une organisation ayant déjà un processus formel de gestion du risque en matière de sécurité de l'information. Le biais favorable des chercheurs pour le processus d'analyse des vulnérabilités comme outil pour améliorer la sécurité de l'information peut avoir un impact sur les résultats.

6.2 Les bases de connaissance

Des recherches ont été effectuées sur les bases de connaissances (KnowledgeBase) de Red Hat, Apache, Symantec et Bugtraq afin d'identifier des vulnérabilités répertoriées. Dans la proposition de travail de synthèse, il avait été prévu d'effectuer ces recherches après les tests de vulnérabilités. Cependant lors de l'exécution du projet il a été jugé plus pratique de les devancer.

Plus de 200 rapports de vulnérabilités ont été identifiés. Cependant plusieurs de ces rapports semblent référer aux mêmes vulnérabilités. Tel que prévu, aucune recherche approfondie n'a été faite sur les probabilités que ces vulnérabilités aient une incidence sur la sécurité du système d'information. Ces résultats ont été présentés aux praticiens. Cette liste de vulnérabilités provenant de sources diverses a reçu un accueil mitigé des participants.

Une discussion entre le chercheur principal et les participants a identifié que les résultats des recherches sont trompeurs. Bien que la quantité d'information semble importante, leur utilité et leur pertinence sont discutables. Les participants ont indiqué qu'ils reçoivent des informations des groupes de discussions et des fabricants de logiciels, mais leur expérience leur a appris qu'il n'est pas prudent de procéder à leur mise en service sans d'abord évaluer la pertinence des changements.

Les praticiens du TCR ont précisé qu'à leur avis, bien qu'il soit vrai qu'un logiciel "plus âgé" est plus connu, et qu'il y a plus de bugs connus, cela ne veut pas dire qu'il est plus propice à des attaques. Dans le cas de mises à jour suggérées, suite à des annonces de fabricants ou reçues via des groupes de discussions, le processus informel en place actuellement est de :

- bien comprendre le problème potentiel de sécurité;
- analyser si le problème a une incidence sur le système d'information;

- appliquer le patch, le service pack ou la mise à jour dans l'environnement de test (labo);

- si l'analyse indique que c'est souhaitable et qu'il n'y a pas de problèmes de compatibilité une mise à jour en production est effectuée.

Il a été déterminé, d'un commun accord avec tous les partis concernés, qu'il n'y avait aucun avantage à présenter ces résultats. Leur utilisation risquerait de confondre les lecteurs de cette étude sur les résultats. Lors de la répétition du processus d'analyse des menaces et des risques, il semblerait préférable d'omettre cette recherche dans les bases de connaissances. L'impact négatif perçu sur la crédibilité du processus par les participants justifie ce retrait.

6.3 L'analyse des risques et des menaces

Dans le cadre de ce travail de synthèse nous avons passé beaucoup de temps à réaliser l'analyse des risques et des menaces. Nous avons pu constater que le dialogue et la recherche d'informations dans un cadre plus formel semblent avoir été perçus comme bénéfiques par les participants. Bien qu'ils soient déjà très sensibilisés aux questions de sécurité de l'information et qu'ils possèdent une vaste expérience en technologies de l'information, ils se disent satisfaits de leur implication dans ce processus. Ils souhaiteraient même réaliser une analyse de ce genre sur l'ensemble de leurs systèmes d'information.

Cependant les praticiens ont exprimé qu'ils préféreraient effectuer des analyses sur un système entier d'information, plutôt que de se limiter à un élément d'actif déterminé. Par exemple, dans le contexte de WebTCR, ceci aurait nécessité l'analyse des serveurs de bases de données, des serveurs Lotus Notes et des interfaces entre ceux-ci. Selon les participants le principal handicap à des analyses de menaces et des risques sur l'ensemble des systèmes d'information est le manque de ressources. Si on considère le temps requis pour l'analyse d'un seul système dans le cadre de notre

travail de synthèse, même avec une optimisation du processus catalysée par l'accroissement des connaissances, il est fort probable que l'analyse de chaque système pourrait demander une importante participation des participants. L'utilisation de ressources externes n'est pas facilement envisageable.

Pour la réalisation de l'analyse des menaces et des risques, nous avons constaté que la présence d'un facilitateur comme le chercheur principal, possédant une bonne compréhension du processus d'analyse de menaces et de risques a été bénéfique. Nous avons constaté que le facilitateur pouvait accélérer le processus en assistant les praticiens dans l'obtention d'un consensus.

Le TCR aurait avantage à identifier et documenter, dans un processus formel, ses besoins en matière de sécurité de l'information. Pour cela il devrait se baser sur les sept objectifs fondamentaux de la sécurité, les recommandations de la CAI, les meilleures pratiques et normes internationales.

Nous avons observé que le système d'information WebTCR est exposé à un niveau de risque faible vis-à-vis l'Internet et moyen à l'intérieur du RTSS. Probablement que si le niveau de risque avait été plus élevé, nos résultats auraient été plus évidents. Nous avons constaté que les principales entraves à l'évaluation du risque et à la sécurité de l'information sont :

- la disponibilité des participants;
- la perception de l'importance du processus;

Par contre nous avons observé que les praticiens du secteur de la santé semblent sensibilisés à la sécurité de l'information, ce qui est confirmé dans la littérature [Smith, 1999][Blobel, 2000].

6.4 L'analyse des vulnérabilités

Les résultats du processus d'analyse des vulnérabilités technologiques, avec l'aide du logiciel Nessus, ont été bien accueillies par les participants. L'impression générale fut que les résultats étaient d'intérêt pour eux. Les praticiens ont d'ailleurs mentionné qu'ils souhaitaient mettre en place la solution Nessus dans leur organisation. Par opposition aux résultats des recherches dans les bases de connaissances, les vulnérabilités ont été mieux acceptées. Il semble que cette acceptation des résultats soit favorisée par les détails techniques, les références à des sources d'informations connues et les pistes de solution offertes.

Les participants ont indiqué, qu'après avoir considéré les extrants du logiciel Nessus, ils perçoivent ce logiciel comme un outil qui pourra leur être utile pour améliorer la sécurité des systèmes d'information du TCR. Nous pouvons observer que le logiciel Nessus par lui-même n'a pas d'impact sur le niveau de risque en matière de sécurité de l'information au TCR. Cependant une meilleure connaissance des vulnérabilités technologiques par les participants apportée par l'utilisation de Nessus est perçue comme une amélioration pour l'organisation.

Les praticiens ont exprimé l'intention de procéder à l'analyse des solutions indiquées dans le rapport. L'éventuelle mise en production d'un serveur, après la mise en place des solutions indiquées, aura comme résultat un serveur plus sécuritaire que le serveur actuel. C'est par la capacité de Nessus d'agir comme catalyseur de changement que nous justifions la perception de l'amélioration.

De par la nature des menaces associées à l'exploitation des vulnérabilités technologiques, il apparaît qu'un état de sécurité perçu comme adéquat par l'organisation peut se détériorer. Il ne suffit que de penser à l'identification de nouvelles vulnérabilités qui évoluent rapidement. De 3 526 en janvier 2002, il y en avait 5366 au début janvier 2003 [NIST, 2002]. Nous croyons qu'en utilisant le

logiciel Nessus de façon régulière au TCR, il sera plus facile de maintenir et d'améliorer le niveau de sécurité de l'information. Cette utilisation régulière pourrait se faire avec la mise en place d'un processus formel d'analyse des vulnérabilités technologiques. C'est ce que les praticiens du TCR qui ont participé au travail de synthèse ont indiqué. Ainsi nous croyons qu'il est correct de penser qu'un processus formel d'analyse des vulnérabilités technologiques est une façon efficace d'améliorer la sécurité de l'information, entre autre en assurant une meilleure protection contre certains types de menaces, dont les cyber-crimes et les menaces reliées aux hackers.

Nous croyons qu'il est cependant important de mentionner les limites du logiciel. Puisqu'il fonctionne en identifiant les vulnérabilités technologiques via le port réseau du serveur analysé, il ne peut identifier que les menaces qui sont 'visibles' de ce point de vue. De plus, à moins de créer ses propres signatures de vulnérabilités technologiques, il n'est possible d'identifier que celles pour lesquelles des signatures sont disponibles. Le logiciel Nessus étant Open Source, le support technique est limité.

Il existe divers produits commerciaux que nous avons testés dans le cadre de la préparation de ce travail de synthèse. Plusieurs de ceux-ci ont une fonctionnalité similaire à Nessus. Nous avons choisi Nessus entre autres pour sa disponibilité, mais nous croyons que nous aurions eu des résultats similaires avec ces autres progiciels.

6.4.1 Utilisation des extrants d'un processus d'analyse des vulnérabilités

Après avoir réalisé l'analyse des vulnérabilités avec Nessus, nous avons discuté des résultats avec les participants. Au TCR, comme c'est le cas dans plusieurs organisations, les praticiens jouent des rôles multiples auprès des divers systèmes d'information de l'organisation. Dans le cas de WebTCR, le développement et la gestion du système sont réalisés par un nombre limité de ressources. Bien que la programmation de certains modules ai été réalisée par une firme de consultants

externes, la configuration et la création des pages html sont réalisées par les praticiens en place. Les principaux intervenants sont les mêmes individus qui ont participé au travail de synthèse. Si l'on considère que le recours aux consultants externes nécessite l'achat de services, le contexte budgétaire en place en limite l'usage. Dans ce contexte ce sont les participants qui effectueraient des modifications au serveur s'ils considèrent qu'une action est souhaitable. Leur prise de décision actuelle correspond au processus informel décrit précédemment. Il serait certainement souhaitable, si l'on se base sur les meilleures pratiques (best practices), que ce processus informel soit formalisé et documenté. Le TCR pourrait considérer l'utilisation de normes reconnues comme ITSM [Assirati, 1999] afin de mettre en place un processus formel de gestion du changement à cette fin. Dans un processus formel, les rapports de Nessus pourraient servir d'élément déclencheur d'un projet de changement aux systèmes d'information.

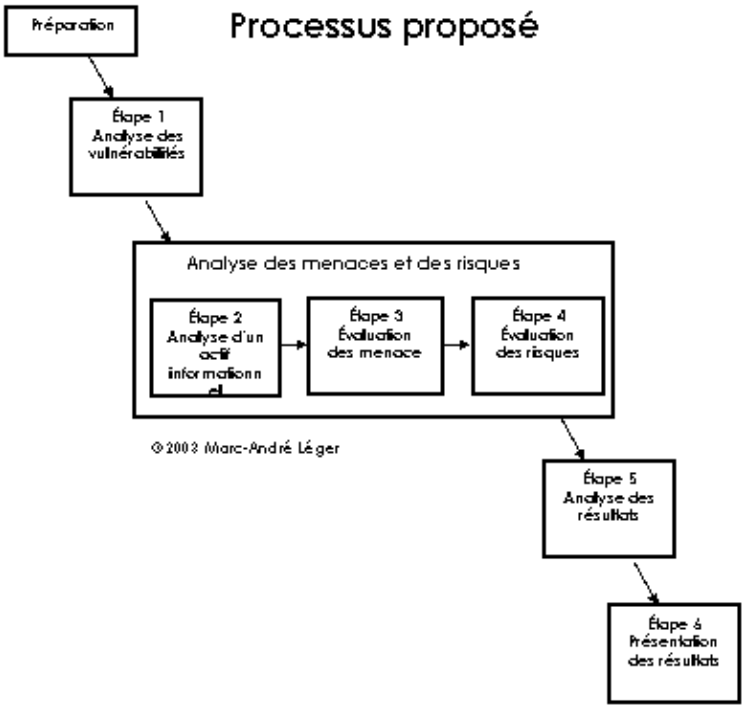

Figure 8 : processus proposé

En l'absence d'un processus formel, dans la situation actuelle, le rapport de Nessus pourrait être acheminé par courrier électronique à un groupe d'individus qui incluraient, dans le cas de WebTCR, les gestionnaires et les praticiens qui ont participé à ce travail de synthèse. L'outil Nessus que nous avons utilisé est intéressant, mais il a des limites. Comme logiciel OpenSource il peut être plus difficile d'obtenir du support. Il est nécessaire d'attendre que des plugins soit disponibles avant d'effectuer une analyse pour une vulnérabilité spécifique. Dans les limites de notre travail de synthèse Nessus s'est avéré utile et efficace. Nous croyons qu'il serait intéressant d'effectuer une analyse comparative des différents outils commerciaux et progiciels disponibles.

6.5 Les processus organisationnels affectés

L'analyse des processus d'affaires de l'organisation, tel que nous souhaitions le faire, devrait être effectuée dans une organisation ayant des rôles et des responsabilités bien identifiés. Le TCR, bien qu'il offre des services multiples à un grand nombre d'utilisateurs, dispose d'une structure organisationnelle souple et qui répond bien à ses besoins. Un nombre très restreint d'individus occupent l'ensemble de tâches diverses durant tout le cycle de vie de l'élément étudié, dont les activités d'évaluation des risques et la mise en productions de modifications aux systèmes.

Comme nous l'avons mentionné précédemment, le TCR n'as pas en place de processus formel de gestion du changement. Le TCR n'a pas non plus de processus formel de gestion du risque. Il semble que c'est l'expertise du personnel en place qui a, dans le passé, permis d'éviter l'exploitation des vulnérabilités du système.

Notre analyse montre que le TCR a en place des mesures de sécurité de l'information qui sont appliquées tout au long du cycle de vie des systèmes d'information. Ces mesures ont été mises en place par les participants sur la base de leur expertise et de leur compréhension des besoins. Pour ce faire, ils se sont appuyés sur les

recommandations de la CAI et du MSSS. La mise en place de ces mesures serait avantagée par un processus formel de gestion du risque, tel que supporté par nos recherches dans les publications récente sur le sujet. Le TCR a l'avantage de disposer de gestionnaires et de praticiens de grande qualité qui ont un souci pour la sécurité de l'information. Il n'y a pas d'incitatifs particuliers pour l'implantation de systèmes d'information sécuritaires. Selon eux, le principal impact de la mise en place d'un système d'information vulnérable, s'il venait a être exposé, serait sur les perspectives de carrière des individus responsables.

Nous avons constaté que le TCR a des processus pour informer le personnel concerné des mesures de surveillance et de contrôle dont il fait l'objet et indiquer l'identité des personnes autorisées à accéder aux informations issues de ces mesures, en précisant les circonstances dans lesquelles elles y accèderont. Nos recherches indiquent que les utilisateurs des données sont sensibilisés aux aspects reliés à la protection des renseignements personnels.

Il n'y a aucun processus formel en place pour contrôler la sécurité des extrants. Cependant les utilisateurs sont tous des professionnels du secteur de la santé sensibilisés aux divers aspects de la sécurité de l'information. Comme professionnels du secteur de la santé, ils sont soumis aux mêmes obligations légales que le TCR mentionnés précédemment dans ce document.

Le TCR a en place des processus et des outils qui lui permettent de se protéger des cyber-attaques. Tout porte à croire que dans le passé le TCR n'a pas fait l'objet de cyber-attaques. L'analyse des menaces et des risques a démontré que le niveau d'exposition au risque de cyber-attaques est moyen. L'analyse des vulnérabilités avec Nessus semble confirmer ce résultat. Ainsi nous avons pu observer qu'il y a des améliorations possibles à ce niveau. De même nous pouvons croire que maintenant que le TCR est informé de ces vulnérabilités spécifiques, il sera en mesure d'apporter des correctifs qui lui permettrons de mieux protéger le serveur des cyber-attaques

provenant tant de l'interne que de l'externe. Le logiciel Nessus se montre utile comme outil pour aider le TCR a rencontrer la recommandation 8.14 du guide de la CAI, soit de mettre en place des mesures pour se protéger des cyber-attaques. Nous avons pu constater qu'il y a des mesures de protections importantes pour isoler le réseau RTSS et par conséquent le TCR des attaques pouvant provenir de l'Internet. En fait, l'utilisation de pare-feux, des zones de sécurité (DMZ) et d'une structure d'adresses privées rendent complexe une cyber-attaques de cette provenance. Une attaque pourrait provenir de branchements depuis le réseau interne.

7 Conclusions

'Si vis pacem, para bellum',

Flavius Vegetius Renatus
~375AD, *De Rei Militari*

Après avoir complété notre recherche, nous croyons qu'il est raisonnable de croire que le processus d'analyse des vulnérabilités, tel que nous l'avons effectué, permet d'accroître le niveau de sécurité de l'information.

Il serait cependant intéressant de considérer un processus où l'analyse des vulnérabilités servirait d'entrée en matière d'un processus plus global d'analyse du risque en matière de sécurité de l'information. En effet, en procédant avec une analyse des menaces et des risques avant de procéder à l'analyse des vulnérabilités, le processus s'est avéré beaucoup plus long qu'il avait été envisagé lors de la proposition de travail de synthèse. Nos observations des résultats du travail de synthèse et la perception par les participants du processus, nous laissent croire que le processus d'analyse des vulnérabilités et le rapport qu'il produit permettrait de procéder plus rapidement dans l'analyse des menaces et des risques. Les données du rapport auraient été utiles pour écourter les discussions sur des menaces envisagées. Ainsi nous pensons que le meilleur usage des rapports produits par l'analyse des vulnérabilités est comme intrant à un processus de gestion du risque en matière de sécurité de l'information.

Nous croyons que notre travail de synthèse démontre l'utilité de l'analyse de vulnérabilités dans l'organisation ciblée. Il semble que des résultats similaires pourraient être obtenus en utilisant un tel outil dans des organisations de moyenne ou grande taille ayant une infrastructure similaire. Considérant le faible coût de mise en place de la solution, il s'agit d'une solution à la portée de tous.

Bibliographie

Alberts, Christopher J., 1999, **Octave Framework version 1.0, technical report**, Carnegie Mellon University, 2001, http://www.atis.org/tg2k/t1g2k.html

Argus, **Les risques informatiques. Les cahiers pratiques**. N°44. Edition l'Argus, septembre 2000. http://sfa.univ-poitiers.fr/commedia/MSTrisq2001/risques-info/synthese.html#Typologies%20des%20risques

Assirati, Bob, **ITIL Security Management**, Central Computer and Telecommunication Agency, Government of the UK, UK, 1999

Barber, B, **Patient data and security: an overview**, international journal of medical informatics, no 49, 1998, pages 19-30

Baskerville, Richard, **Investigating Information Systems with Action Research**, Communications of the association for information systems, Volume 2, article 19, Octobre 1999, http://www.cis.gsu.edu/~rbaskerv/CAIS_2_19/CAIS_2_19.html

Berryman, Paul, **Risk Assessment: The Basics**, Mémoire présenté comme exigence partielle pour l'obtention de la certification de Global Information Assurance Certification du GIAC, http://www.giac.org/, Février 2002

Bierman, Elmarie, **Classification of malicious hosts threats in mobile agent computing**, Proceedings of SAICSIT 2002, pages 141-148

Blobel, Bernd, **Advanced toolkits for EPR security**, International journal of medical informatics, no 60, 2000, pages 169-175

Boudreau, Christian et la CAI**, Étude sur l'inforoute de la santé au Québec : Enjeux techniques, éthiques et légaux, document de réflexion**, octobre 2001

CAIDA, the Cooperative Association for Internet Data Analysis, **Caida analisys of Code Red,** http://www.caida.org/analysis/security/code-red/, 2002

Canada, 1985, **Code criminel du Canada (L.R. 1985, ch. C-46)** art 342.1, 342.2, 430.

Cash, J. et al, **Corporate information systems management: text and cases**, Irwin, Boston,Third edition 1992

CERT, Securing Networks Systematically --- the SKiP Method, CERT ® Coordination Center, Carnegie Mellon University, 2002(1)

CERT, **CERT® Advisory CA-2001-19 "Code Red" Worm Exploiting Buffer Overflow In IIS Indexing Service DLL**, Carnegie Mellon University, CERT Coordination Center advisory, http://www.cert.org/advisories/CA-2001-19.html, 2001

CERT, **CERT® Advisory CA-2002-22 Multiple Vulnerabilities in Microsoft SQL Server**, Carnegie Mellon University, CERT Coordination Center advisory, http://www.cert.org/advisories/CA-2002-22.html, Juillet 2002

CERT, **CERT® Advisory CA-2003-04 MS-SQL Server Worm**, Carnegie Mellon University, CERT Coordination Center advisory, http://www.cert.org/advisories/CA-2003-04.html, Janvier 2003

Commission d'accès à l'information du Québec, Exigences minimales relatives à la sécurité des dossiers informatisés des usagers du réseau de la santé et des services sociaux, Avril 1992

Commission d'accès à l'information du Québec,Avis concernant le cadre g;lobal de gestion sur la sécurité des actifs informationnels du réseau de la santé et des services sociaux, décembre 2001

Commission d'accès à l'information du Québec, Guide en matière de protection des renseignements personnels dans le développement des systèmes d'information à l'intention des ministères et organismes publics, Décembre 2002

COSISS, **Politique intérimaire de sécurité visant les actifs informationnels du réseau de la santé et des services sociaux**, Québec, 1999.

CSI, Computer Security Institute, **Cyber crime bleeds U.S. corporations, survey shows; financial losses from attacks climb for third year in a row**, Avril 2002

Denning, Dorothy E., **Cyberterrorism**, Global Dialogue, Autumn, Aout 2000

Denning, D,.**Hacktivism: An Emerging Threat to Diplomacy**, Foreign Service Journal, September 2000.

Forristal, J, **Vulnerability Assessment Scanners**, http://www.networkcomputing.com/1201/1201f1b1.html, Janvier 2001

Gendarmerie Royale du Canada, **Guide d'évaluation de la menace et des risques pour les technologies de l'information**, Novembre 1994

Godbout, L'Honorable Juge Bernard, j.c.s., jugement de la cause Wellman c. Québec (Ministère de la Sécurité du revenu-secrétariat) Cour Supérieure, Québec, District de Chicoutimi, N°:150-05-000416-950, 19 juillet 2002

Gordon, Laurence A. et Loeb, Martin, **The economics of Information security investment**, ACM Transactions on information and system security, vol 5, no 4, Novembre 2002, pages 438-457

Haimes, Yacov Y. (1999), **The Role of the Society for Risk Analysis in the Emerging Threats to Critical Infrastructures** , Risk Analysis, Blackwell Science, UK, April 1999, Volume 19, Issue 2, pages 153-157

Hancock, Bill, COMMON SENSE GUIDE FOR SENIOR MANAGERS, Top Ten Recommended Information Security Practices, 1st Edition - July 2002

Harvey, P.L., Cybersciences (Québec Sciences), juin 1997, http://www.cybersciences.com/Cyber/1.0/1_29_116.asp

Hult, M., **Towards a Definition of Action Research: a Note and Bibliography**, Journal of Management Studies, 1980, pages 241-250.

IDefence, Code Red FAQ v1.0, http://www.idefense.com/Intell/CI081001.html, 2002

International Standards Organisation (ISO**), ISO/EIC TR 13335-1, Information technology – Guidelines for the management of IT Security, Part 1: Concepts and models for IT security**, décembre 1996

Janczewski, Lech, and Shi, Frank Xinli, **Development of Information Security Baselines for Healthcare Information Systems in New Zealand,** Computers & Security, Volume 21, Issue 2, 31 March 2002, pages 172-192

Johansson, Jesper M., **2.1 Code Red worm exploits idq.dll buffer overflow,** SANS Windows Security Digest, vol. 4 No. 7 - Juillet 2001

Jordan, Tim**, A sociology of hackers,** the sosiological review, 1998, pages 757-780

Kalla, M. et als, **Achieving non-repudiation of web based transactions**, The journal of systems and software, 1999

Kremer, S. et als, **An tensive survey of non-repudiation protocols**, Computer Communications, no 25,2002, pages 1606-1621

Landwehr, Carl E., **Formal models for computer security**, ACM Computing serveys, vol 13, no 3, Septembre 1981pages.247-278

Maiffret, Marc, **Bugtraq announcement of Code Red**, http://online.securityfocus.com/archive/1/191873/2001-06-12/2001-06-18/0

Maguire, Stuart (2002), **Identifying risks during information system development: managing the process**, Journal of Information Management & Computer Security, Volume 10 Number 3, pages 126-p134

Martin, Robert A. , **Managing Vulnerabilities in Networked Systems,** IEEE computer, p 32-38, Novembre 2001

Microsoft, **Microsoft Security Bulletin MS01-033 Unchecked Buffer in Index Server ISAPI Extension Could Enable Web Server Compromise**, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS01-033.asp, Juin 2001

Microsoft, **Microsoft Security Bulletin MS02-039Buffer Overruns in SQL Server 2000 Resolution Service Could Enable Code Execution (Q323875)**, Juin 2002, http://www.microsoft.com/technet/treeview/default.asp?url=/technet/security/bulletin/MS02-039.asp

Moore, David, **Code-Red: a case study on the spread and victims of an Internet worm**, Presented at the Internet Measurement Workshop (IMW), Cooperative Association for Internet Data Analysis – CAIDA, San Diego Supercomputer Center, University of California, San Diego, 2002

Moore, David et als, CAIDA, the Cooperative Association for Internet Data Analysis,The **Spread of the Sapphire/Slammer Worm**, février 2003, http://www.caida.org/outreach/papers/2003/sapphire/sapphire.html

MSSS, Ministère de la Santé du Québec, **Le réseau RTS C'est**, site internet du MSSS, http://www.msss.gouv.qc.ca/rtss/, 2003

MSSS, Ministère de la Santé du Québec, **Le réseau de télécommunication sociosanitaire en bref**, document interne du TCR, 2002

NIST, ICAT Metabase, Vulnerability Statistics, http://icat.nist.gov/icat.cfm?function=statistics, avril 2002

Poulsen, Kevin, **Terrorism Talks**, Open RSA Conference, http://online.securityfocus.com/news/336 , Février 2002

SANS Institute, **The Twenty Most Critical Internet Security Vulnerabilities, The Experts' Consensus**, May 2002, http://www.sans.org/top20.htm

Scott-Morton M., **The Corporation of the 1990s: Information Technology an Organisational Transformation**, Oxford University Press, 1991

Smith, Alan D, Rupp William T (2002), **Issues in cybersecurity; understanding the potential risks associated with hackers/crackers**, Journal of Information Management & Computer Security, Volume 10 Number 4, Pages 178-183

Smith, E. Eloff, J.H.P., **Security in health-care information systems – current trends**, International journal of medical informatics, no 54, 1999, pages 33-54

Sweltz ,Ken, Network Vulnerability Assessment Strategy for Small State and Local Government Agencies, SANS Institute, GIAC practical repository, 2003

Tregear, Jonathan, Risk Assessment Information Security Technical Report , Volume 6, numéro 3, septembre 2001, pages 19-27