Vérification du système de gestion de l'information sur les heures de travail (système TIME)

Produit pour le compte de :	**l'Office national de l'énergie** **444, Septième Avenue S.-O.** **Calgary (Alberta) T2P 0X8**
Produit par :	**TRM Technologies Inc.** **151, rue Slater** **Pièce 100** **Ottawa (Ontario) K1P 5H3**
Date :	**15 octobre 2004**
N^{o} de contrat :	**84084040098**

Remerciements

La réalisation du présent projet n'aurait pas été possible sans le concours des membres du personnel de l'Office national de l'énergie. TRM Technologies tient à remercier sincèrement tous ceux qui ont fourni la documentation et l'information nécessaires pour mener à bien son mandat et qui ont participé aux entrevues de recherche des faits.

Nos remerciements s'adressent également au responsable du projet, M. Albert Fung, pour son aide dans l'organisation des entrevues et la collecte d'information.

FICHE D'APPROBATION

Produit par : M. Harrop B.Sc. en ingénierie, MBCS
Conseiller principal, sécurité des TI

B. Falvo
Conseiller, sécurité des TI

Revu par : _____
R. Moxley PEng.
Directeur, sécurité des TI

Approuvé par :_____
T. F. Martin PEng.
Président, TRM Technologies

Acronymes et abréviations

PCA	Plan de continuité des affaires
CCC	Comité consultatif sur le changement
SBR	Services de bureau et de réseau (équipe de l'ONÉ)
PRA	Plan de reprise après sinistre
CFA	Certificat de fiabilité approfondie
EXTRA	Extranet de l'ONÉ (système d'accès à distance)
SIRH	Sytème d'information sur les ressources humaines
SIUI	Services d'information sur l'utilisation d'Internet
TI	Technologie de l'information
STI	Sécurité des technologies de l'information
ONÉ	Office national de l'énergie
OP	Ordinateur personnel
EFVP	Évaluation des facteurs relatifs à la vie privée
MDS	Méthodologie de développement des systèmes
END	Énoncé de la nature délicate
SQL	Langage relationnel SQL
SCT	Secrétariat du Conseil du Trésor
EMR	Évaluation des menaces et des risques

TABLE DES MATIÈRES

Résumé

La présente vérification du système de gestion de l'information sur les heures de travail (Time Information ManagEment System – TIME) a été lancée sur l'initiative du Comité de vérification et d'évaluation de l'Office national de l'énergie pour s'assurer que les contrôles de traitement en place sont suffisants et que l'information sur les heures de travail est exacte et remise dans les délais pour les fins de la gestion. Le mandat comportait deux volets : d'une part, un examen approfondi du système TIME, de son contexte d'exploitation et des consignes de sécurité à l'aune des Directives du Gouvernement du Canada sur la vérification de la sécurité, des exigences des politiques et d'autres guides de pratiques exemplaires; d'autre part, un examen indépendant du code du programme en vue de relever les vulnérabilités sur la base des directives de Microsoft en matière de sécurité et des pratiques exemplaires recommandées en matière d'applications .NET.

La vérification a permis d'établir qu'il n'existe pas de faiblesses majeures dans les contrôles de traitement du système TIME, mais que certains aspects méritent l'attention si l'on veut réduire les problèmes potentiels. Les principales conclusions sont résumées ci-après.

Sécurité des systèmes : La protection du réseau et du système TIME est généralement efficace, comme l'illustrent la vérification et l'examen de la sécurité menés en 2003/2004 sous l'égide du Comité de vérification et d'évaluation (réf. 2.2). Aucune preuve n'a été trouvée qui pourrait laisser croire que de nouvelles vulnérabilités du réseau ont été introduites depuis l'examen précédent. Les mesures de protection du réseau de l'ONÉ sont pleinement suffisantes pour protéger le système TIME.

Continuité du service : Même si un plan de reprise après sinistre (PRA) a été élaboré pour l'infrastructure des TI de l'ONÉ, il n'a pas encore été mis en œuvre et il n'existe pas de dispositions de rechange pour le système TIME en cas de panne grave. Cette question nécessite l'attention, non pas seulement pour le système TIME, mais aussi pour l'ensemble du traitement de l'information à l'ONÉ.

Gestion des risques : En général, les processus de gestion des risques sont adéquats, sauf qu'aucun énoncé de la nature délicate (END) n'a été élaboré pour les données du système TIME, ce qui signifie que les décisions en matière de risques sont prises sans disposer d'une information suffisante. Une évaluation des menaces et des risques (EMR) a été entreprise pour le système TIME mais nous n'avons pas été en mesure de confirmer que les recommandations ont été mises en œuvre.

Gestion des données : Les procédures de gestion et de protection des données sont généralement suffisantes et efficaces, comme le sont les procédures de sauvegarde et les couplages des données avec les autres systèmes. Toutefois, en l'absence d'un énoncé de la nature délicate, il est possible que les données ne soient pas entièrement protégées en conformité avec les exigences du Gouvernement du Canada.

Gestion des incidents : Les procédures relatives à la gestion des problèmes et des incidents sont jugées suffisantes et efficaces.

Gestion de la configuration : Les dispositions actuelles relatives à la gestion de la configuration à l'ONÉ sont pleinement suffisantes en ce qui concerne le système TIME. Les dispositions établies pour le réseau et les TI de l'ONÉ répondent pleinement aux besoins du système TIME en matière de protection physique et environnementale.

Gestion des changements : Les changements apportés au système TIME sont contrôlés et gérés comme il se doit. La planification de la sécurité des TI et la participation au processus de développement du système TIME sont jugées suffisantes et efficaces. Des problèmes pourraient surgir un jour en ce qui concerne le traitement des changements d'urgence, mais des recommandations sont faites pour y remédier.

Conception et codage du système : Plusieurs vulnérabilités associées au codage du programme. NET ont été relevées mais seulement deux d'entre elles (la vulnérabilité par injection SQL et l'exposition aux attaques sur les éléments dynamiques) sont considérées comme présentant un risque élevé. Des recommandations sont incluses pour remédier à la situation.

Autres questions : Le rapport signale plusieurs autres vulnérabilités potentielles, mais la probabilité qu'elles soient exploitées est jugée faible. Même si la production des relevés par les employés s'est considérablement améliorée, des préoccupations sont quand même exprimées à l'égard des déclarations tardives et de la capacité de vérifier l'exactitude des données transmises très tardivement.

Le système TIME est un outil efficace de production de relevés et de gestion des heures de travail. La mise à jour, la déclaration et l'examen dans les délais prescrits sont maintenant chose possible et l'identification des problèmes est plus facile que sous l'ancien système. L'exactitude des données est rehaussée du fait que les relevés sont remis à temps et, dans l'ensemble, la qualité des données devrait s'en trouver grandement améliorée par rapport à l'ancien système. La sécurité des données est au moins aussi bonne que sous l'ancien régime. De plus, le système TIME a permis la mise en oeuvre de nouvelles politiques sur la production des relevés. Même si certains relevés sont produits en retard, le système aide à exercer un meilleur contrôle et devrait permettre à l'ONÉ de baser le recouvrement des frais sur des informations plus actuelles.

Les vulnérabilités potentielles et les sujets de préoccupation sont tous exposés dans les *Conclusions* du rapport. Onze recommandations ont été faites qui, si elles sont mises en

oeuvre, remédieront aux vulnérabilités potentielles et amélioreront la sécurité du système en général.

1. Contexte et introduction

1.1 Le système TIME

Le système de gestion de l'information sur les heures de travail (ou système TIME) de l'Office national de l'énergie est un système en ligne qui facilite la déclaration et la gestion de l'utilisation des heures de travail des employés par type d'heures (heures normales, congés, heures supplémentaires, crédits d'heures de travail, etc.), par projet, par produit et par but général de l'ONÉ. Le système prévoit l'entrée et l'autorisation des relevés de temps chaque semaine, et il sert à faciliter le recouvrement des frais selon le type de produit. Le système prévoit également le suivi des coûts des immobilisations. La direction s'en sert pour suivre et approuver l'utilisation des heures de travail par les employés et pour soutenir certains processus des secteurs. Le système peut servir à élaborer des rapports sur l'emploi du temps.

Le système TIME a été mis au point à l'interne pour remplacer un système provisoire de feuilles de calcul en Excel de Microsoft. La phase I du système TIME, qui a été lancée en juin 2002, comportait des fonctions de base de déclaration des heures pour répondre aux besoins en matière de recouvrement des frais. Plusieurs améliorations ont été apportées depuis le lancement de la Phase I pour accroître la fonctionnalité globale et l'utilité du système.

Le système TIME mis au point à l'interne en 2002 est codé au moyen de la technologie .NET de Microsoft; il utilise une base de données Server 2000 en langage relationnel SQL. Il est lié au système d'information sur les ressources humaines (SIRH) par une application Bridge (elle aussi mise au point à l'interne) et il est accessible aux utilisateurs par l'intranet de l'ONÉ à l'aide d'un navigateur. Le système est également accessible aux employés hors place par l'extranet (EXTRA) de l'ONÉ.

1.2 Objectifs et portée de la vérification

La vérification avait pour but premier de s'assurer que les contrôles des processus du système TIME sont suffisants et efficaces pour assurer le maintien de l'intégrité et de la disponibilité des données relatives aux présences et absences des employés de l'ONÉ. Il s'agissait de mener d'une part un examen approfondi des contrôles des processus du système d'information, en conformité avec les pratiques de sécurité exemplaires généralement acceptées et les Directives du Gouvernement du Canada sur la vérification de sécurité, et d'autre part une évaluation détaillée de la conception et du code du système, afin de repérer les éventuelles vulnérabilités et les variations par rapport aux pratiques exemplaires de sécurité qui régissent les applications .NET.

Étaient exclues de la vérification de sécurité les réseaux de données, les gardes-barrière, les routeurs et les autres ressources de réseau qui ne sont pas propres au système TIME. En étaient également exclues les méthodes d'exploitation du système en tant que telles et les installations de secours hors-site, de même que les systèmes auxiliaires (comme

l'application Bridge et le SIRH) qui ont une interface avec le système TIME ou qui lui fournissent des données.

Un examen et une vérification approfondis de la sécurité des technologies de l'information (TI) à l'ONÉ ont été entrepris fin 2003, début 2004 (réf. 2.2) et une Évaluation des menaces et des risques qui pèsent sur le système TIME a été réalisée en 2003 (réf. 2.6). Nous n'avons pas cherché à reproduire ou à réévaluer quelque constatation que ce soit découlant de ces évaluations, mais les résultats ont été pris en considération dans la mesure où ils avaient une incidence sur le système TIME.

2. Méthodologie

2.1 Démarche et méthodologie

La méthodologie employée pour la vérification reposait sur diverses techniques, notamment des visites et des examens sur place et hors place, l'examen de la documentation existante (y compris le code réel), l'examen des résultats des inspections et évaluations antérieures, des entrevues avec le personnel clé et l'évaluation par rapport aux méthodes reconnues de sécurité et de vérification de la sécurité des TI.

Le travail a été réparti en trois phases :

Phase 1 : Planification et examen initial

- Procéder à un examen initial de l'environnement de la gestion de l'information et du système TIME.
- Passer en revue les exigences du Gouvernement du Canada en matière de vérification et d'inspection de la sécurité des systèmes de TI et déterminer celles qui étaient pertinentes à la vérification.
- Élaborer une liste de contrôle de vérification à partir des points ci-dessus.
- Élaborer une approche d'évaluation du système TIME (conception et code).
- Procéder à un examen initial de la documentation préliminaire remise avant la visite du site et relever les lacunes constatées dans la documentation.

Phase 2 : Visite du site et examen approfondi du système

- Interviewer le personnel clé.
- Relever les lacunes constatées dans la documentation ou dans d'autres documents pertinents.
- Procéder à un examen approfondi de la documentation disponible sur le système TIME, notamment l'information de base et les lois, politiques et procédures pertinentes et la documentation relative au système TIME.
- Obtenir des éclaircissements sur des questions découlant des entrevues et des documents.
- Assister à une démonstration en direct du système et de ses capacités.

- Procéder à un examen détaillé du code et des contrôles du système.
- Élaborer une approche détaillée pour la phase d'analyse et de déclaration.

Phase 3 : Analyse, évaluation et déclaration

- Évaluer l'information recueillie au cours des phases 1 et 2, et, si nécessaire, chercher de l'information supplémentaire.
- Analyser et évaluer l'information recueillie en ce qui concerne la vérification et les contrôles de sécurité des TI.
- Relever les lacunes, s'il y en a.
- Documenter les constatations dans un rapport de vérification qui contiendra des recommandations destinées à remédier aux lacunes relevées.
- Présenter les résultats au responsable du projet à l'ONÉ sous forme de rapport préliminaire.
- Examiner (et revoir si nécessaire) le rapport préliminaire après examen par l'ONÉ et élaborer le rapport final.

Tel qu'indiqué dans l'énoncé de travail et dans le plan d'action, les éléments du système TIME pris en compte dans la présente vérification étaient : la continuité du service, la sécurité des systèmes, la gestion de la configuration, la gestion des problèmes et des incidents, la gestion des données et la gestion des changements. Ont également été prises en considération la gestion des risques et les autres questions.

2.2 Évaluation de l'application TIME

L'évaluation du programme TIME comprenait une démonstration de l'application, une revue générale du système et de l'infrastructure de développement en compagnie d'un des développeurs, et une analyse détaillée de la conception et du code. Des pages, des éléments personnalisés et des objets-application ont été identifiés pour comprendre l'approche du développement.

Ensuite, le code a été examiné pour évaluer tous les aspects de l'application où la sécurité pourrait poser problème, en particulier les techniques de développement, les mesures de prévention, le déploiement et la configuration.

2.3 Cadre d'exploitation du système TIME

L'examen du cadre et des méthodes d'exploitation du système TIME consistait à évaluer tous les aspects liés au système proprement dit, ses données et ses interactions, dans le contexte global d'exploitation de l'ONÉ.

Tous les documents disponibles ont été examinés : documents de conception, formats des rapports, règles administratives, méthodes d'exploitation, messages d'erreur, sondages sur la satisfaction des utilisateurs, procédures de conversion, documents d'essai et résultats des essais. Des entrevues ont été menées auprès du personnel clé et des questions de suivi ont été envoyées par courrier électronique et par téléphone.

Les critères d'évaluation provenaient des sections pertinentes du Guide de vérification - Sécurité des technologies de l'information du Conseil du Trésor, d'autres guides de vérification de sécurité et de pratiques exemplaires (réf. 3.3, 3.4, 3.5 et 3.6, surtout), et des exigences applicables aux systèmes individuels en matière de politique de sécurité et de pratiques exemplaires.

La mesure dans laquelle le système TIME satisfait (ou ne satisfait pas) aux critères a été évaluée à partir des entrevues réalisées et des documents fournis, et d'une évaluation des caractéristiques de programmation et de conception du système.

3. Constatations

3.1 Fonctionnalité du système TIME

Le processus de gestion du temps qui a précédé le système TIME, le contrôle des procédures intérimaires de déclaration du temps (connu sous l'acronyme anglais TRIP), était une mesure à court terme élaborée dans le cadre du passage à l'an 2000. Il reposait sur l'entrée manuelle des données au moyen d'une feuille de calcul en Excel. Le processus comportait de nombreuses étapes et bien souvent les données étaient enregistrées en retard. Qui plus est, les données des feuilles de calcul s'altéraient, rendant impossible l'enregistrement exact des heures de travail. C'était un processus à la fois coûteux et inefficace et c'est pourquoi le déploiement du *système* TIME a été accéléré pour tenter de régler ces problèmes.

Avec le système TIME, chaque employé est tenu de déclarer ses heures de travail de la semaine précédente au plus tard le mardi matin. Lorsqu'un relevé de temps en ligne n'a pas été soumis, un rappel par courriel est envoyé dès le lendemain. Le chef d'équipe concerné est avisé des relevés de temps qui n'ont pas été soumis après une semaine. Tous les relevés de temps non soumis figurent également sur la Liste des choses à faire du chef d'équipe. (Actuellement, la notification ne va pas au-delà du palier du chef d'équipe.) En général, le délai de soumission des relevés de temps est bien plus observé sous le système TIME.

L'administrateur du système TIME produit des rapports trimestriels faisant état du nombre de relevés de temps non reçus par secteur.

Les possibilités d'erreurs d'enregistrement des heures sont limitées (et pas plus nombreuses que dans le cas des rapports sur support papier). Par exemple, un employé peut faire une erreur en consignant ses heures travaillées, ses heures supplémentaires, ses congés ou ses crédits d'heures, mais il appartient à son chef d'équipe de vérifier qu'elles ont été enregistrées correctement. Lorsque les relevés de temps sont soumis dans les délais, il est beaucoup plus probable que les erreurs d'enregistrement seront découvertes.

L'accès aux données du système TIME est accordé selon le poste occupé. Les employés n'ont accès qu'à leurs propres données. Les chefs d'équipe ont accès aux données de leurs employés aux fins de la vérification, de l'approbation et de la planification.

Il revient aux chefs d'équipe d'examiner et d'approuver les données d'entrée, les congés et les heures supplémentaires déclarés. Le personnel des ressources humaines et les chefs d'équipe se servent de ces données pour préparer les rapports sur les RH. Le personnel des RH s'en sert également pour soutenir les enquêtes.

Le système TIME a certes aidé à régler un bon nombre de problèmes liés à la qualité des données et au respect des délais de soumission des relevés qui étaient le lot de l'ancien système. Les sondages auprès des employés effectués après la mise en œuvre du système

TIME révèlent un degré élevé d'acceptation et de satisfaction des utilisateurs à l'égard du système.

3.2 Efficacité des contrôles de traitement du système TIME

3.2.1 Continuité du service

Actuellement, il n'existe pas de plan de continuité des affaires (PCA), ni de plan d'urgence, ni de procédures de reprise après sinistre pour le système TIME. Un plan de reprise après sinistre (PRA) a été élaboré pour l'infrastructure des TI de l'ONÉ dans son ensemble, mais il n'a pas encore été mis en œuvre. *Il n'y a pas de mesures de traitement de rechange dans l'éventualité d'une panne grave du système.* Cela mérite une attention particulière, non pas seulement pour le système TIME mais pour l'environnement tout entier du traitement de l'information à l'ONÉ.

Les données du système TIME sont sauvegardées et enregistrées sur bande magnétique chaque jour à partir du serveur. Les bandes sont expédiées chaque mois à Bibliothèque et Archives Canada qui les conserve pendant 26 mois. Les procédures actuelles de sauvegarde et de récupération pour le serveur SQL, ainsi que la fréquence des sauvegardes, répondent entièrement aux besoins du système TIME.

L'incidence d'une panne grave du système TIME dépendrait de la durée et de la gravité de la panne. Une panne de moins de sept jours aurait probablement une faible incidence (p. ex., il y aurait vraisemblablement quelque retard dans la soumission des relevés de temps) mais l'incidence s'amplifierait sans doute avec la durée de la panne. Il n'existe aucune disposition pour se rabattre sur les processus papier : ainsi, les relevés de temps seraient simplement retenus jusqu'à la remise en état du système.

Alors que d'autres systèmes seraient vraisemblablement affectés dans une plus grande mesure que le système TIME lors d'une panne de système grave, l'absence d'un PCA et d'un PRA opérationnels représente une sérieuse faiblesse en plus de ne pas atteindre les objectifs du gouvernement en ce qui concerne la continuité de la prestation des services.

3.2.2 Sécurité des systèmes

Dans une très large mesure, les besoins du système TIME en matière de sécurité sont satisfaits au moyen de processus et de procédures mis en place par les Services de bureau et de réseau (SBR) en vue d'assurer la sécurité du réseau de l'ONÉ, des postes de travail et du service d'accès à distance.

<u>Procédures pour contrôler l'authentification, l'autorisation et l'accès au système TIME</u>

Le système TIME a été conçu pour permettre l'authentification et l'autorisation de l'utilisateur afin de lui garantir l'accès légitime à sa base de données. Les règles d'authentification et d'accès sont régies par les exigences du réseau de l'ONÉ en la matière et aussi par les exigences propres au système TIME. L'accès à celui-ci se fait par la connexion normale intranet de l'ONÉ ou par la connexion extranet (EXTRA). L'authentification électronique est assurée au moyen d'un accès protégé par mot de passe dans le cas de l'intranet et par des jetons et des mots de passe dans le cas de l'EXTRA.

L'accès au TIME est limité aux employés de l'ONÉ qui sont tenus d'avoir un certificat de fiabilité approfondie (CFA). L'accès au réseau est accordé par le personnel des SBR à la demande du surveillant de l'employé et l'accès est révoqué selon les formalités de départ. Le contrôle d'accès est basé sur les rôles et la répartition des tâches : les droits d'accès sont déterminés en fonction du poste ou du rôle de l'utilisateur. Les règles d'accès, qui sont définies dans les règles administratives (réf. 2.11), régissent la gestion des codes de projet.

Lorsqu'un employé est absent, l'administrateur du système TIME peut déléguer ses droits d'accès après avoir consulté le chef d'équipe concerné. Certains cadres de direction ont également accès par délégation à leur adjoint administratif. Lorsqu'un employé occupe un poste par intérim (rémunéré ou non), l'accès peut être délégué et la délégation est consignée dans le SIRH. L'accès du titulaire qui occupe le poste par intérim est maintenu pendant une semaine après le retour du titulaire en titre afin de permettre la vérification des relevés de temps couvrant la dernière semaine d'absence du titulaire.

Mis à part l'accès aux fins de la déclaration (accordé à tous les employés) et de la gestion, il existe des droits d'accès spéciaux pour certains employés des Finances (aux fins de la déclaration et du recouvrement des frais), certains employés désignés des systèmes (pour introduire les codes d'accès critiques), le conseiller en RH (pour les relations avec le personnel et les enquêtes, notamment pour examiner le profil des congés de maladie). De plus, l'administrateur du système et trois membres du personnel des RH y ont accès pour administrer le système et extraire les données des rapports et les introduire (manuellement) dans le SIRH. (L'administrateur du système ne peut pas modifier les données d'un relevé de temps mais il peut les effacer complètement.) Par ailleurs, l'adjoint administratif du chef des opérations a accès au système pour examiner les relevés des heures non compensatoires.

L'accès externe au système TIME se fait par l'EXTRA au moyen de jetons RSA et du protocole SSL par l'entremise d'un serveur CITRIX. L'accès est régi par un mot de passe et un NIP. On dénombre actuellement 150 jetons et 140 comptes actifs. Une évaluation des menaces et des risques (EMR) qui pèse sur l'EXTRA a été effectuée en septembre 2003 et on ne signale aucune question non résolue ni aucune vulnérabilité qui pourrait avoir une incidence sur le système TIME. (Nous n'avons pas examiné les résultats de cette évaluation car cela n'entrait pas dans le cadre de notre mandat.) Une norme a été élaborée pour l'EXTRA afin de régir les mécanismes d'identification et d'authentification et une politique a été élaborée pour en régir l'utilisation.

En général, les processus de révocation sont efficaces. L'accès au réseau est révoqué selon les formalités de départ. L'accès peut également être révoqué pour d'autres motifs sur une base individuelle. L'accès au réseau par les employés contractuels est limité à la période du contrat (bien que seuls les employés de l'ONÉ aient accès au système TIME).

Les procédures et les contrôles régissant l'authentification, l'autorisation, l'accès et la révocation sont jugés entièrement satisfaisants pour le système TIME.

Actualisation et communication des politiques et procédures

Les procédures régissant l'utilisation du système TIME sont énoncées dans le document publié dans l'intranet TIME 3.0 Help (réf. 2.3), qui indique également les mises à jour du système. Le document d'aide (Help) est un outil exhaustif efficace pour guider les utilisateurs et informer le personnel des changements courants apportés. Il s'agit du moyen de communication principal entre le personnel chargé du développement du système TIME et ses utilisateurs, bien que le courrier électronique soit également utilisé de temps à autre.

Dans l'ensemble, la documentation sur les procédures est jugée efficace et suffisante.

Politiques et procédures sur la sécurité logicielle

Les dispositions sur la sécurité logicielle applicable au système TIME sont contenues en partie dans la méthodologie de développement des systèmes (MDS) et plus généralement dans le cadre de la politique de sécurité de l'ONÉ, ainsi que dans les politiques applicables du SCT et de l'ONÉ sur les ressources humaines. Collectivement, elles fournissent des balises suffisantes aux concepteurs, aux programmeurs et aux utilisateurs pour maintenir le niveau de sécurité logicielle approprié.

Politiques et procédures de sécurité des communications

L'utilisation du système TIME se fait exclusivement par l'intranet ou l'EXTRA.

Les procédures de sécurité du réseau de l'ONÉ répondent entièrement aux besoins du système TIME et on constate un bon niveau de conformité avec ces procédures.

Utilisation des mesures de protection du réseau

Des mesures de protection du réseau appropriées ont été mises en place et les membres du personnel sont très conscients de la nécessité d'une protection efficace du réseau. Tout le travail en réseau se fait à l'interne, sauf pour l'accès à distance dont il a été question plus haut.

Un garde-barrière géré par les Services gouvernementaux de télécommunications et d'informatique (SGTI) permet d'isoler le réseau interne et les données du réseau public Internet. Tout le trafic sur le réseau et aux postes de travail est soumis au balayage contre les virus et les codes malveillants; les utilisateurs de l'EXTRA sont tenus par principe d'installer des logiciels antivirus et des gardes-barrière sur tout système utilisé pour accéder à distance à l'EXTRA.

Les mesures de protection du réseau de l'ONÉ sont pleinement efficaces pour protéger le système TIME.

3.2.3 Gestion des risques

Suffisance de l'information pour prendre des décisions sur les risques

Aucun énoncé de la nature délicate (END) n'a été élaboré pour les données du système et aucune évaluation des facteurs relatifs à la vie privée (EFVP) n'a été effectuée. Cela serait imputable au fait que les données n'ont pas changé avec le passage du support papier au support électronique. Il n'y a pas eu non plus d'END (ni d'EFVP) lorsque le processus se faisait sur support papier.

Comme il n'y a pas d'END ni d'EFVP, il n'existe pas suffisamment d'information pour prendre des décisions sur les risques.

Le personnel de l'ONÉ présume que les données du système TIME sont désignées Protégé B ou moins, mais il sait également que certaines données personnelles sont extrêmement sensibles. Même si les dispositions relatives au traitement répondent au niveau de protection requis pour les données Protégé B, sans un END, il y aura toujours un degré d'incertitude quant à la sensibilité des données. Un END établirait une base pour s'assurer que les données sont protégées et manipulées comme il se doit.

Suffisance du cadre et des méthodes de gestion des risques pour la STI à l'ONÉ

L'ONÉ utilise le processus simplifié d'évaluation des risques (Facilitated Risk Assessment Process, ou FRAP), qui permet le contrôle par les pairs pendant le développement du système. Mis à part l'absence d'un END, la sécurité a été assurée de manière suffisante pendant l'étape du développement du système TIME et le coordonnateur de la sécurité des TI a été consulté aux étapes préliminaires du projet.

Il n'y a aucune exigence particulière en matière d'entretien de la sécurité du système TIME, hormis celles précisées dans les documents Politique et cadre de sécurité à l'ONÉ et méthodologie de développement des systèmes (MDS).

Lorsque le système TIME a été mis au point en 2002, la MDS ne comprenait pas d'exigences particulières en matière de sécurité ou de protection de la vie privée. La sécurité était assurée en consultant le coordonnateur de la sécurité des TI et était conçue pour répondre aux besoins de fonctionnement. La MDS a beaucoup évolué depuis. Le développement des systèmes et les processus d'examen font dorénavant obligation de tenir compte des exigences de sécurité durant les étapes de la conception et du développement.

Dans l'ensemble, le processus de gestion des risques de sécurité est considéré comme suffisant et efficace pour le système TIME. Le processus de développement, même s'il ne suit pas entièrement une MDS unique reconnue, est jugé approprié, compte tenu du statut de la MDS au moment du développement initial.

Évaluation des menaces et des risques (EMR)

Une EMR du système TIME a été effectuée en 2003 (réf. 2.6), dont les résultats ont été passés en revue lors d'une présentation interne en janvier 2004 (réf. 2.7). *On nous a dit que l'EMR n'avait révélé aucune question non résolue ni aucune vulnérabilité, mais nous n'avons pu confirmer, par les entrevues ou les documents, que tous les risques relevés avaient été circonscrits.* De plus, il y a eu des changements au niveau du personnel du système TIME responsable de la mise en œuvre de ces recommandations. Il est suggéré de procéder à un examen plus approfondi des constatations de l'EMR, afin de confirmer que toutes les vulnérabilités relevées ont été prises en considération comme il se doit.

Tel qu'indiqué plus haut, une EMR des systèmes connexes a été effectuée sur le réseau EXTRA en 2003. *Par contre, ni le SIRH ni le système Bridge n'ont fait l'objet d'une EMR*.

3.2.4 Gestion des données

Les données du système TIME sont stockées sur place dans une grappe SQL gérée par CGI Inc. La validation des données à la source est effectuée à plusieurs niveaux. Les relevés de temps ne peuvent pas être soumis s'ils ne respectent pas les règles administratives (réf. 2.11). Il existe un contrôle pour protéger le système contre les combinaisons de données invalides (p. ex., on ne peut pas saisir des crédits d'heures de travail durant une période de congé de maladie). Les erreurs associées à l'exactitude des données (p. ex., les heures soumises) ne peuvent être décelées que par les chefs d'équipe qui vérifient si les données sont vraisemblables et ne contiennent pas d'erreurs flagrantes.

Lors de la mise en oeuvre du système et de l'abandon du système des feuilles de calcul en Excel, les administrateurs des données ont validé toutes les données et communiqué avec les employés lorsqu'ils trouvaient des données douteuses. Tous les employés étaient priés de vérifier les données de leur relevé (tel que précisé dans les documents d'essai).

Les données TIME sont conservées indéfiniment dans le système TIME et sont sauvegardées hors place.

Couplage des données

Les données du système TIME sont exclusivement à caractère interne. Aucune donnée n'est automatiquement échangée avec d'autres systèmes.

Le principal couplage se fait avec le système d'information sur les ressources humaines (SIRH) qui a des données communes à toutes les applications RH (p.ex., nom, poste, surveillant et périodes d'absence). Les données de base utilisées par le système TIME se trouvent dans le SIRH mais il n'y a pas de lien direct entre le TIME et le SIRH. L'information qui circule entre les deux est unidirectionnelle, c.-à-d. que les données passent exclusivement du SIRH au TIME; aucune donnée ne circule directement du

TIME au SIRH. L'information est transférée par le biais d'une application Bridge, un système développé à l'interne et qui sert d'autres systèmes, en plus du TIME. Si le SIRH ou le Bridge tombait en panne, il n'y aurait pas de connexion en ligne permettant d'obtenir les nouvelles données des employés.

À cause des flux limités des données et parce que les couplages fonctionnels sont exclusivement à caractère interne, le risque qui pèse sur le système TIME à partir de ces couplages est jugé faible. *Toutefois, ni le Bridge ni le SIRH n'ont fait l'objet d'une EMR.*

Protection des données

L'autorisation des transactions et l'accès aux données sont régis par les dispositions du système définies dans le document *Roles, Responsibilities and Permissions* (réf. 2.3.). D'un point de vue opérationnel, seul un nombre limité d'employés a accès au système qui permet de changer les autorisations. (Il s'agit essentiellement de l'administrateur du système, et éventuellement du programmeur de la maintenance du logiciel). En général, les employés n'ont pas accès aux écrans, sauf autorisation. Le système comporte un contrôle automatique qui veille à ce que les données consignées soient « plausibles » (p. ex., que le système n'autorise pas certaines combinaisons de données); le système ne permettra pas la saisie de données s'il détecte des avertissements spécifiques, mais il appartient aux chefs d'équipe de contrôler l'exactitude des heures déclarées.

La gestion et l'examen du compte de l'utilisateur relèvent de l'administrateur du système, bien que le chef d'équipe, Systèmes d'information, ait accès au système TIME pour saisir les codes d'accès cruciaux. Les privilèges d'accès au système TIME sont établis par le groupe des TI à la demande de l'administrateur du système TIME. Ces processus sont potentiellement vulnérables, en particulier si quelqu'un a obtenu l'accès au compte de l'administrateur du système, mais le fait que l'accès au système soit limité aux employés de l'ONÉ et qu'il se fait exclusivement par l'intranet de l'ONÉ ou l'EXTRA ramène le risque à un niveau gérable. Toutefois, il est extrêmement important que ceux qui ont un accès privilégié conservent soigneusement leurs mots de passe et utilisent des mots de passe non triviaux. L'accès à l'aide de jetons (plutôt que par mots de passe) pour les utilisateurs à accès privilégié réduirait davantage le risque associé à la compromission des mots de passe.

Les données du système TIME sont considérées comme étant désignées Protégé B ou moins, mais on n'a effectué ni d'END ni d'EFVP pour confirmer la sensibilité des données. *Contrairement à la politique établie, les données ne sont pas marquées, même lorsqu'elles figurent dans un rapport imprimé.* C'est sans doute en raison de l'incertitude qui entoure la classification de la sensibilité. Dans l'environnement du serveur, le traitement est effectué dans des installations qui s'occupent de données désignées Protégé B au moins. Les copies de secours du système sont marquées Protégé B au moyen d'étiquettes spéciales.

3.2.5 Gestion de la configuration

Le système TIME fonctionne selon la configuration standard poste de travail/réseau de l'ONÉ. Lorsqu'il faut apporter des modifications à la configuration, celles-ci sont analysées et approuvées par le Comité consultatif sur le changement[1] (CCC) et documentées dans le lecteur F, sous Secteur de la gestion de l'information.

Lors de la mise en œuvre du système TIME, la configuration de certains ordinateurs de bureau a posé des problèmes, qui ont tous été résolus après la période initiale de deux mois. Le logiciel fonctionne maintenant sur tous les systèmes.

Les dispositions actuelles en matière de gestion de la configuration sont pleinement suffisantes pour le système TIME.

Normes de sécurité physique et de l'environnement

Le système TIME n'a pas d'autres normes de sécurité physique ou de l'environnement que celles qui concernent l'environnement global, le réseau et l'accès à l'extranet de l'ONÉ. Les normes de sécurité physique et de l'environnement ont été prises en compte dans la conception et le développement du réseau et de l'extranet. De plus, la participation du coordonnateur de la sécurité des TI au processus d'examen de la conception du système TIME a permis de répondre aux besoins particuliers dans ce domaine.

Les dispositions établies pour le réseau et les TI de l'ONÉ répondent entièrement aux besoins en matière de sécurité physique et de l'environnement du système TIME.

3.2.6 Gestion des changements

Planification de la sécurité des TI

Tel qu'indiqué dans la réf. 2.2, l'ONÉ a en place une infrastructure de gestion de la sécurité efficace.

La planification de la sécurité des TI et la participation au processus de développement du système TIME sont jugées suffisantes et efficaces.

[1] Les membres du CCC sont le DPI, le coordonnateur de la sécurité des TI et les chefs d'équipe des Systèmes d'information et des Services de bureau et de réseau.

Maintenance du système

Il n'est pas question de développer davantage le système TIME, si ce n'est que pour y apporter des changements pour mieux l'adapter.

Les procédures de maintenance du système, d'amorçage de changements et de contrôle sont exposées dans les procédures du CCC (réf. 2.12). Les procédures de maintenance sont mal définies dans la MDS, alors que les rôles liés à la maintenance sont définis. En ce qui concerne les révisions ou les mises à niveau prévues du système, une évaluation des répercussions est effectuée par la personne qui propose le changement. La proposition est alors présentée au CCC, qui l'examine et la valide s'il y a lieu. Toutes les propositions de changement entérinées par le CCC sont conservées dans le lecteur F.

Les procédures de documentation des changements exigent que les commentaires soient insérés avec le code. Les améliorations de même que le numéro de la version sont résumés dans le fichier d'aide (Help).

Un système de pré-production permet de tester les changements à apporter au système de production. Une fois les changements approuvés et testés, le transfert à l'environnement de production est approuvé par le CCC. En général, on ne procède pas à l'examen des codes avant l'étape de la production, sauf de la part du programmeur d'origine, sauf que le code du système TIME a été examiné au cours de la présente vérification.

Il n'existe pas de politique de diffusion des logiciels à proprement parler. Les changements au système TIME sont apportés au fur et à mesure des besoins, même si en général les changements non urgents sont groupés puis diffusés sur une base trimestrielle. Les changements urgents sont mis en oeuvre immédiatement après consultation informelle des personnes en cause.

Même si ce processus semble bien fonctionner, nous avons relevé deux problèmes potentiels. Premièrement, l'autorisation du CCC n'est nécessaire que pour les changements majeurs. Les mises à jour mineures et les changements urgents ne sont pas signalés au CCC et sont soumis à un contrôle informel seulement. Les changements urgents sont codés et testés par le programmeur puis testés par l'administrateur du système TIME. Ils ne sont pas soumis au CCC et la seule documentation consiste en des courriels explicatifs entre le développeur/programmeur, le personnel de production et l'administrateur du système TIME. Deuxièmement, le code du système TIME renferme des commentaires uniquement pour une partie du code. Ces questions ne causent pas de problèmes pour l'heure, mais elles pourraient finir par en causer en cas de changements de personnel ou s'il se révélait un jour nécessaire de revoir l'historique des révisions antérieures.

Le processus de mise à jour soulève également des préoccupations, particulièrement en ce qui concerne les changements non planifiés. L'environnement de production est verrouillé de sorte que les développeurs n'y ont pas accès. Lorsqu'il est nécessaire d'accéder à l'environnement de production (p. ex., pour exécuter un script de

développement), le développeur demande à un membre du personnel de production d'exécuter le script. Les scripts sont généralement livrés sur une disquette et le membre du personnel de production reçoit de brèves explications sur ce que le code doit faire. Toutefois, la demande et le script ne sont consignés nulle part. Jusqu'à présent, seuls deux employés ont été associés au processus. Par ailleurs, ce processus ne semble pas documenté dans des procédures formelles. Le processus reste donc très informel et repose sur la confiance mutuelle des employés concernés. L'absence de toute documentation sur la demande ou le script pourrait causer des problèmes importants, surtout s'il y avait des changements au niveau du personnel.

3.2.7 Gestion des problèmes et des incidents

Si le système tombe en panne ou que des problèmes sont décelés, le bureau de service est le premier point de contact. Il tient un journal des incidents dans le système HEAT. Les incidents touchant le réseau sont pris en charge par le personnel des SBR. Les incidents touchant le système TIME sont référés au groupe de développement responsable. La réponse dépend de la nature de l'incident. Le coordonnateur de la sécurité des TI est informé des incidents liés à la sécurité.

Il n'existe pas de piste de vérification du système TIME à proprement parler, mais il existe des données de suivi qui peuvent servir à produire un historique de chaque relevé de temps (qui a fait quoi et quand). Des timbres-dateurs sont faits à chaque mise à jour du système et un enregistrement des changements apportés au système est effectué. (Comme il a été dit plus haut, cet enregistrement ne comprend pas les données sur les changements urgents.)

Le traitement des incidents passe par plusieurs niveaux. L'identification automatisée des événements opérationnels est assurée par Big Brother qui en qualifie l'impact potentiel au moyen de la cote élevée, moyenne ou faible. Un examen manuel systématique des journaux des événements est effectué sur le serveur afin de déceler tout comportement anormal. Un système de détection d'intrusion (logiciel Tripwire) est en voie d'être mis en œuvre. En ce qui concerne les contrôles administratifs, tous les employés sont tenus de n'utiliser que leur propre compte et de verrouiller leur poste de travail dès qu'ils s'absentent.

Les attaques contre le système TIME par des utilisateurs autorisés (des employés) ne sont pas considérées comme une menace grave. Le type d'incident le plus probable (les déclarations erronées de la part des employés) serait très probablement décelé par les procédures d'examen et de déclaration intégrées dans le système. À ce jour, les exemples de mauvais usage du système par les employés sont rares. Les incidents décelés sont soumis aux procédures disciplinaires normales.

Les procédures de gestion des problèmes et des incidents sont jugées efficaces.

3.2.8 Autres questions

Aucun incident relatif à la sécurité du système TIME n'a été signalé jusqu'ici. Les principales préoccupations soulevées par le personnel de l'ONÉ au cours des entrevues concernaient les risques potentiels qui pèsent sur l'intégrité et la cohérence des données du système. *Le plus grand risque qui pèse sur l'intégrité des données est celui de la tentative d'altération, même si l'on juge peu probable que cette menace se concrétise.* Ceux qui sont autorisés à accéder au système TIME ont peu de motivation à manipuler les données de façon malveillante.

Les attaques d'origine externe supposent qu'on pénètre le système par le garde-barrière ou qu'on utilise un système compromis pour y accéder. Des mesures de protection contre ce type d'attaque sont en place, savoir des mesures standard de protection du réseau de l'ONÉ, mais la motivation à perpétrer une attaque de l'extérieur contre les données du système TIME est jugée faible.

Il est possible pour un employé qui s'y connaît d'accéder au système par une trappe. Un tel accès pourrait entraîner des changements aux droits d'accès (p. ex., si le système Bridge était compromis, il serait possible pour un utilisateur averti de changer la structure de la déclaration). Là aussi, la motivation à mener une attaque de ce genre est jugée faible.

Le système TIME est la première application .NET/SQL développée pour l'ONÉ. Cela se reflète dans une certaine mesure dans sa conception car une partie des méthodes de l'ancien système a été reprise dans le nouveau.

Il est possible que les droits d'accès soient mal configurés par le fait de processus manuels, mais il est plus probable que cela soit dû à des erreurs de saisie plutôt qu'à une attaque délibérée.

Même si le système a grandement amélioré le processus de soumission des rapports dans les délais, les déclarations tardives posent encore problème. Il est difficile pour les chefs d'équipe de vérifier l'exactitude des données qui parviennent très tard. Il semble difficile de convaincre les employés de l'importance de soumettre leurs données à temps. Peut-être est-ce dû au fait que le personnel ne comprend pas vraiment la fonction première du système TIME, qui est de faciliter le recouvrement des frais.

3.3 Examen de la conception et du codage du système TIME

Cette partie de la vérification concerne la conception et le code de programme du système TIME, qui a été développé en Visual Studio.NET. L'application est évaluée sur la base des recommandations du guide de sécurité .NET de Microsoft. Les risques potentiels de sécurité ont été analysés dans le cadre du code de programme, de son environnement d'hébergement et de l'environnement des données. Tous les aspects vulnérables le plus fréquemment trouvés dans les applications du Web développées en ASP.NET ont été

examinés. Enfin, les configurations du serveur SQL et des SII ont été examinées pour confirmer que les normes de sécurité y ont été suivies.

Cette partie du rapport fournit une brève description des fonctions employées pour assurer la sécurité de chacun des aspects du système soumis à examen. Viennent ensuite des observations particulières sur les fonctions du système TIME. Lorsque des vulnérabilités potentielles en matière de sécurité sont relevées, des recommandations sont faites afin d'atténuer les risques.

3.3.1 Techniques cryptographiques

Des techniques cryptographiques sont utilisées pour transformer les données afin d'en protéger la confidentialité et/ou l'intégrité. Il y a d'abord le chiffrement, qui consiste à cacher les données en vue d'en protéger le contenu à l'aide d'un algorithme cryptographique réversible, puis il y a les fonctions de condensation qui servent à produire un condensé cryptographique irréversible d'information afin d'en confirmer l'intégrité. Microsoft Windows et .NET Framework renferment des algorithmes cryptographiques robustes.

Le système TIME n'a pas besoin de faire un grand usage de la cryptographie. De par la nature de l'application, il n'est pas nécessaire de chiffrer les données transmises par le client. Le système TIME fait un usage approprié du chiffrement par clé secrète pour éviter d'exposer à tout risque les comptes validés des utilisateurs et les mots de passe donnant accès aux bases de données.

3.3.2 Authentification et autorisation ASP.NET

L'authentification confirme l'identité de la personne, alors que l'autorisation contrôle les opérations qu'un utilisateur peut exécuter.

Le système TIME fait un usage approprié du logiciel Integrated Security de Windows pour authentifier les utilisateurs et leur donner accès à l'application. Tous les utilisateurs ayant un compte Windows pour le domaine ont accès au système TIME. Si un utilisateur tente de lancer TIME sans passer par le réseau, il lui sera demandé d'entrer un numéro d'utilisateur et un mot de passe pour un domaine spécifique.

Le processus d'authentification du système TIME nécessite l'authentification de Windows et la confirmation que l'utilisateur existe dans la base de données commune.

Le système TIME n'utilise pas les capacités intégrées ASP.NET pour autoriser les utilisateurs authentifiés. Il utilise plutôt une forme de programme d'autorisation sur mesure. C'est une approche sûre et recommandée qui offre une fonctionnalité semblable aux capacités ASP.NET.

Même si le système TIME utilise les capacités d'authentification de Windows, il ne tire pas profit des contrôles d'accès intégrés basés sur les rôles. Il gère plutôt ses propres rôles

à l'aide de composantes établies sur mesure. Le support intégré ASP.NET des contrôles d'accès basés sur les rôles aurait simplifié l'autorisation dans certains cas et pu réduire de beaucoup les efforts consentis pour le codage. Cela étant dit, la technique employée ne crée pas de vulnérabilités pour la sécurité.

3.3.3 Attaques sur l'application

En général, les attaques sur les réseaux partagés ou sur les systèmes et applications Internet sont lancées à deux niveaux différents : au niveau du système et au niveau de l'application. Dans la présente vérification, nous nous sommes penchés sur les attaques dirigées contre l'application et sur les aspects où les applications .NET sont vulnérables aux attaques.

Attaques par injection SQL

Une application est vulnérable aux attaques lorsque les données non vérifiées de l'utilisateur sont utilisées dans le cadre d'une chaîne de données présentées en langage relationnel (SQL) qui est construite pour former l'énoncé SQL final. Le langage SQL intégré est employé dans l'ensemble du code de l'application TIME.

Attaques sur les éléments dynamiques

Le système TIME n'utilise aucune des techniques de codage HTML ou URL mais il fait amplement usage des appels en SQL intégré avec des chaînes de données présentées en langage SQL construites avec des variables contenant des données de l'utilisateur non contrôlées. Cela, ajouté au fait que le système TIME a été développé et compilé dans .NET 2002, fait en sorte que le TIME est vulnérable aux attaques sur les éléments dynamiques. Par défaut, les systèmes compilés avec .NET 2003 sont protégés contre toute attaque sur les éléments dynamiques.

L'application TIME est extrêmement vulnérable aux attaques par injection SQL et aux attaques sur les éléments dynamiques.

On peut utiliser diverses techniques pour éviter que le système TIME soit vulnérable aux attaques par injection SQL et sur les éléments dynamiques.

Techniques défensives contre les attaques par injection SQL

Il existe plusieurs moyens de se prémunir contre une attaque par injection SQL. Au minimum, le système TIME devrait valider les paramètres d'entrée et utiliser les interrogations paramétrées. De plus, il faudrait considérer l'utilisation des procédures stockées comme l'approche recommandée. Toutefois, comme le langage relationnel intégré SQL a été utilisé dans l'ensemble de l'application, il serait tout aussi efficace et moins fastidieux de valider les paramètres d'entrée et d'utiliser les interrogations paramétrées.

Techniques défensives contre les attaques sur les éléments dynamiques

Il existe des techniques simples pour se prémunir contre les attaques sur les éléments dynamiques. Les données présentées dans une page HTML peuvent être protégées à l'aide du *Server.HTMLEncode*. Les données utilisées dans une page URL, comme par exemple une valeur de chaîne d'interrogations passées à une autre page Web, peuvent être protégées à l'aide du *Server.UrlEncode*. De plus, le contenu et la longueur des données peuvent être validés au moyen des contrôles de validation ASP.NET.

Les applications Web codées dans .NET 2003 sont automatiquement protégées contre les attaques sur les éléments dynamiques. La conversion et le déploiement de l'application TIME sous forme de produit .NET 2003 réduiraient sensiblement les vulnérabilités actuelles aux attaques sur les éléments dynamiques.

3.3.4 Validation des données

ASP.NET comporte des contrôles pour valider à la fois le client et le serveur mais l'application TIME fait très peu usage des validateurs de contrôle ASP.NET. Elle fournit une forme de validation côté serveur alors que la validation côté client devrait servir de première ligne de défense. Les validateurs de contrôle ASP.NET sont là pour faciliter la validation côté client avant que les données de l'utilisateur ne soient transmises au serveur. Ce type de validation permet d'éviter les allers-retours inutiles vers le serveur pour fournir les messages d'erreur de validation causés par des valeurs d'entrée mal formées.

Le système TIME fournit la validation côté serveur pour l'événement à l'origine de la demande. Les valeurs d'entrée sont ensuite validées dans la logique du code puis traitées comme il se doit. Cette méthode de validation ne donne lieu à aucun risque de sécurité.

Même si les méthodes de validation actuellement employées dans le système TIME ne présentent pas de vulnérabilités pour la sécurité, il faudrait utiliser les contrôles de validation ASP.NET lorsqu'il y a lieu. Ces contrôles sont simples à implanter et servent de mesure de défense même si la logique du code s'occupe elle-même de la validation. À tout le moins, les contrôles de validation pourraient aider à réduire au minimum la quantité de code requise par les routines de validation côté serveur.

3.3.5 Traitement des exceptions

Même si les logiciels sont conçus pour fonctionner dans un environnement agencé pour pouvoir fonctionner à la perfection, il reste que l'environnement en question est moins que parfait et que tout peut dérailler. Du point de vue de la sécurité, les failles d'un logiciel sont non seulement une nuisance mais elles peuvent présenter des vulnérabilités susceptibles d'être exploitées par un intrus qui pourrait attaquer le logiciel ou le système sur lequel il est exécuté.

La conception d'un logiciel destiné à traiter les exceptions sans difficulté vise deux objectifs : se protéger des attaques et permettre une expérience plus robuste et plus satisfaisante pour l'utilisateur. Des exceptions peuvent survenir n'importe où dans le code, mais la plupart du temps elles surviennent lorsqu'il se présente une situation non prévue par le développeur et que la logique du programme ne permet pas de traiter les données sans difficulté.

Le traitement des erreurs dans le système TIME n'entraîne pas de vulnérabilité pour la sécurité. Des routines locales sont mises en place dans la plupart des procédures afin de traiter les exceptions non prévues. Le système TIME possède une routine globale pour le traitement des exceptions qui surviennent suite à des circonstances imprévues. Il utilise la fonction .NET pour renvoyer automatiquement l'utilisateur à une page d'erreurs génériques lorsque surviennent des exceptions non piégées. Cette page d'erreurs indique également le type d'exception et des informations détaillées sur les erreurs pour les utilisateurs jouissant d'un accès privilégié.

Globalement, l'application TIME s'acquitte bien de sa tâche de traiter les exceptions locales et globales; cet aspect du code d'application n'a pas besoin d'être réexaminé.

3.3.6 Verrouillage de Windows, des SIUI et de .NET

Le verrouillage de Windows, des Services d'information sur l'utilisation d'Internet (SIUI)) et de .NET sert à limiter les services utilisés par l'application et à apporter des changements à la configuration pour désactiver les services inutilisés. La plate-forme doit être verrouillée car même si elle est sécurisée, l'installation implicite ne l'est pas nécessairement.

Microsoft fournit trois outils automatisés pour verrouiller Windows et les SIUI, mais ils ne sont pas utilisés actuellement.

Aucun des outils automatisés de verrouillage n'a été utilisé dans le système TIME pour verrouiller Windows ou les SIUI. Ces outils, bien qu'ils ne soient pas absolument nécessaires, aident vraiment à identifier les risques potentiels pour la sécurité.

Même si le système TIME n'est pas directement exposé à l'Internet public, il est recommandé d'utiliser les outils automatisés pour pouvoir verrouiller Windows et les SIUI afin d'éliminer un certain nombre de risques résiduels. Cette opération demande un effort minime.

Microsoft recommande également de toujours isoler les contrôles de domaine. Pour le système TIME, il ne s'agit pas d'une menace sérieuse car la plupart des vulnérabilités résiduelles pour la sécurité sont le fait de personnes oeuvrant au sein de l'organisation. On évitera toutefois d'avoir un contrôleur de domaine qui fournit également d'autres types de services de réseau, comme les services d'impression, les bases de données et les SIUI.

3.3.7 Sécurisation de la base de données

Les concepts à la base de la sécurité des bases de données sont exactement les mêmes que pour la sécurité d'une application, savoir : authentifier, autoriser et verrouiller. Plusieurs mesures peuvent être prises pour améliorer la sécurité du serveur SQL. Voici lesquelles.

Les services SQL devraient être exécutés sous un compte d'utilisateur de domaine à faibles privilèges pour s'assurer que, si jamais un intrus réussissait à s'infiltrer et à s'emparer du serveur SQL, il serait limité à un compte de domaine à faibles privilèges.

Si un intrus obtient l'accès au serveur SQL et est autorisé à exécuter xp_cmdshell, il peut faire tout ce que le compte de service du serveur SQL est autorisé à faire. Pour cela, il est recommandé de supprimer *xp_cmdshell* à moins d'absolue nécessité.

La fonction Vérification indique si quelqu'un essaie de pénétrer la base de données, mais actuellement elle n'est pas activée. Il est recommandé de choisir l'option de niveau de vérification *All (Tous)*.

3.3.8 Conclusion globale sur l'examen de la conception et du codage du système TIME

De tous les risques relevés dans la présente section de la vérification, seuls deux sont réellement considérés à haut risque. Le reste peut être considéré à faible risque. Comme le système TIME est une application intranet qui est déjà bien protégée du monde extérieur par un garde-barrière et d'autres mesures de sécurité du réseau, le niveau de menace pour la plupart des vulnérabilités mentionnées dans le rapport est passablement faible.

Les deux vulnérabilités pour la sécurité qui méritent vraiment une attention particulière sont : la vulnérabilité par injection SQL et l'exposition aux attaques sur les éléments dynamiques. Cette dernière peut facilement être contrée par une mise à niveau du système TIME avec .NET 2003. Quant à la vulnérabilité par injection SQL, il faudrait y mettre un peu plus d'efforts mais cela se ferait assez facilement.

4. Conclusions générales et recommandations

Le système TIME fournit à l'ONÉ un outil efficace de gestion et de déclaration des heures de travail. La mise à jour, la déclaration et l'examen des données dans les délais sont maintenant possibles et l'identification des problèmes est plus facile que sous l'ancien système. D'autre part, le système a permis la mise en oeuvre de nouvelles politiques de déclaration. Bien que des retards subsistent toujours, le système offre un meilleur contrôle global et devrait permettre à l'ONÉ d'établir le recouvrement des frais sur la base de données plus actuelles. De plus, l'exactitude des données s'en trouve améliorée du fait que les relevés sont davantage soumis dans les délais et, globalement, la qualité des données devrait s'en trouver grandement améliorée.

La sécurité des données est au moins aussi bonne que sous l'ancien système. Le risque global pour l'intégrité du système TIME et des données est réduit au minimum car on évite l'exposition au réseau public Internet. Un certain nombre de points méritent une attention particulière mais la vérification n'a pas permis d'identifier des faiblesses majeures dans les contrôles du processus.

En ce qui concerne la conception et le codage, deux vulnérabilités assez graves ont été relevées: la vulnérabilité par injection SQL et l'exposition aux attaques sur les éléments dynamiques. Il serait également possible d'améliorer la sécurité sur plusieurs points en ajustant le code ou en installant une version plus récente de .NET. Ces points sont résumés dans le corps du texte.

Toutes les vulnérabilités potentielles et tous les sujets préoccupants sont mis en italique dans la section *Constatations* du rapport. Les recommandations qui suivent, si elles étaient mises en oeuvre, permettraient de contrer ces vulnérabilités potentielles et d'améliorer la sécurité globale du système. Les recommandations sont présentées par ordre de priorité.

Recommandation 1 : Il est recommandé de mettre en oeuvre des procédures afin de prémunir le système contre les attaques par injection SQL. À tout le moins, il faudrait valider les paramètres d'entrée et utiliser des interrogations paramétrées.

Recommandation 2 : Il est recommandé de mettre en oeuvre des procédures afin de prémunir le système contre les attaques sur les éléments dynamiques. On peut utiliser *Server.HTMLEncode* pour protéger les données présentées dans une page HTML. On peut également utiliser *Server.UrlEncode* pour protéger les données utilisées dans une page URL, comme par exemple une valeur de chaîne de données d'interrogation passée à une autre page Web. De plus, le contenu et la longueur des données peuvent être validés à l'aide des contrôles de validation ASP.NET. Il faudrait penser à installer une version .NET 2003 et à la déployer dans l'application TIME. Cela permettrait de réduire sensiblement les vulnérabilités aux attaques sur les éléments dynamiques.

Recommandation 3 : Il est recommandé de prendre aussitôt que possible des mesures pour mettre en oeuvre les dispositions sur la continuité des affaires, en particulier le Plan de reprise après sinistre.

Recommandation 4 : Il est recommandé de préparer un énoncé de la nature délicate (END) pour les données du système TIME qui servirait d'assise pour protéger et traiter les données de manière appropriée. Toutes les données sensibles devraient être accolées d'inscriptions sensibles conformément à l'END. Même si cela déborde du cadre spécifique de la présente vérification, il est recommandé de préparer un END pour les données du SIRH également.

Recommandation 5 : Comme des changements ont été apportés à la composition du personnel responsable de la suite à donner aux constatations de l'EMR du système TIME et qu'il n'est pas clair que suite a été donnée à toutes les constatations, il est recommandé

d'examiner les constatations de l'EMR pour s'assurer que toutes les vulnérabilités ont été prises en considération.

Recommandation 6 : Il est recommandé de mettre en oeuvre des procédures pour s'assurer que tous les changements apportés au système TIME (y compris la maintenance non prévue) sont bel et bien documentés. Les documents comprennent le script réel, l'heure et la date auxquelles la demande a été faite pour exécuter le script, le nom de la personne à l'origine de la demande de changement et le nom du membre du personnel de production qui opère le changement.

Recommandation 7 : Il est recommandé d'activer les outils automatisés pour pouvoir verrouiller Windows et les SIUI (Services d'information sur l'utilisation d'Internet). Il est également recommandé d'isoler les contrôleurs de domaine.

Recommandation 8 : Pour rehausser la sécurité de la base de données, il est recommandé que les services SQL soient exécutés sous un compte d'utilisateur de domaine à faibles privilèges. Il est également recommandé de supprimer *xp cmdshell* à moins d'absolue nécessité. Enfin, il est recommandé de procéder à la vérification du langage relationnel SQL (c.-à-d., qu'il faudrait choisir l'option de niveau de vérification SQL *All (Tous)*.

Recommandation 9 : Il est recommandé de penser à utiliser les fonctions d'autorisation intégrées de Windows et en particulier le support ASP.NET pour les contrôles d'accès basés sur les rôles.

Recommandation 10 : Même si les méthodes de validation actuellement associées au système TIME ne posent pas de menaces pour la sécurité, il est recommandé que les contrôles de validation ASP.NET soient utilisés lorsqu'ils sont jugés appropriés. Ces contrôles sont très simples à implanter et constituent une mesure de défense accrue même si la logique du code s'accommode bien de la logique de la validation. À tout le moins, les contrôles de validation pourraient aider à réduire au minimum la quantité de code requise par les routines de validation côté serveur.

Recommandation 11 : Même si cela déborde du cadre de la présente vérification, il est recommandé de procéder à une évaluation des menaces et des risques pour les systèmes Bridge et SIRH (Système d'information sur les ressources humaines).

Références

1. Politiques, méthodes et procédures du gouvernement du Canada et du Conseil du Trésor

1.1 Sécurité des technologies de l'information – Guide de vérification, SCT, 1996
1.2 Politique sur la sécurité, SCT, février 2002
1.3 Politique sur l'autorisation et l'authentification électroniques, SCT, juillet 1996

2. Politiques, méthodes et procédures de l'ONÉ

2.1 Politique et procédures de sécurité, juillet 2001
2.2 Vérification et examen de la sécurité des technologies de l'information, TRM Technologies, 15 janvier 2004
2.3 TIME V3.0 Help
2.4 TIME Project Charter
2.5 TIME Project Management plan v.3.0
2.6 TIME TRA (tableur Excel)
2.7 Présentation : TIME TRA Review, 12 janvier 2004.
2.8 TIME report mock ups (28 fichiers au total)
2.9 TIME report use case (10 fichiers au total)
2.10 SQL Server Backup and Recovery Review
2.11 System TIME Business Rules
2.12 Change Advisory Board Procedures

3. Autres documents de référence

3.1 Proposal for the Audit of the Time Information ManagEment (TIME) System, TRM
3.2 Technologies, 17 juin 2004
3.3 Action Plan for NEB System TIME audit, août 2004
3.4 Management Planning Guide for Systems Security Auditing, National State Auditors and US General Accounting Office, décembre 2001
3.5 Site Security Audit Checklist, G Halprin, SysAdmin Group, juin 2003
3.6 Computer Security Audit Checklist, C.Rose, ITSecurity.com, avril 2002
3.7 Computer Security Audit Checklist, Chris Hardie, Summersault.com, avril 2003

Personnes interviewées

Les membres du personnel de l'ONÉ suivants ont été interviewés dans le cadre de la présente vérification :

Albert Fung, directeur, Vérification et évaluation
Jeanette Johnston, administratrice du système TIME
Howard Plato, chef d'équipe, Services de bureau et de réseau
Kevin Campbell, coordonnateur, Sécurité des technologies de l'information
Mike Knopp, analyste et programmeur, système TIME
David Young, chef d'équipe, Systèmes d'information
Elke Meyer, analyste de la gestion du changement, gestionnaire de projet, Phase 1 du système TIME