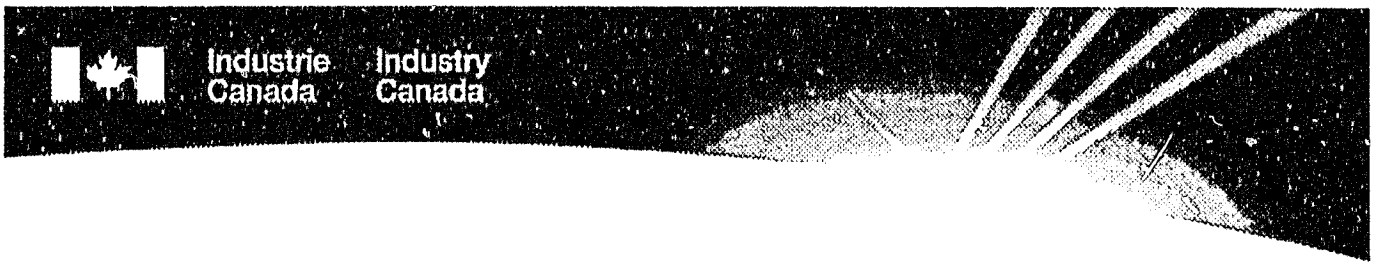

VÉRIFICATION
DE LA
SÉCURITÉ DU RÉSEAU LOCAL (LAN)
DE LA DIRECTION DES CORPORATIONS

16 septembre 1997

Direction générale de la vérification et de l'évaluation

Canada

TABLE DES MATIÈRES

SOMMAIRE

La Direction générale de la vérification et de l'évaluation a mené une vérification des contrôles relatifs au réseau local (LAN) de la Direction des corporations durant le premier trimestre de l'exercice financier de 1997-1998. Cette vérification a été planifiée et approuvée dans le plan de la Direction générale de la vérification et de l'évaluation de 1997-1998.

La Direction des corporations a mis en oeuvre de nombreux contrôles solides qui minimisent les risques à la sécurité. Toutefois, dans un environnement de systèmes changeants, la sécurité peut présenter certaines failles. Le présent rapport identifie les contrôles efficaces utilisés, ainsi que les domaines où la Direction des corporations peut renforcer la sécurité des systèmes.

Contrôles efficaces

Les contrôles efficaces énumérés ci-dessous servent à renforcer la sécurité des systèmes car la Direction des corporations a assuré que :

- les employés qui quittent la Direction sont immédiatement supprimés de la liste des comptes LAN autorisés, ce qui réduit le risque d'un accès non autorisés au LAN;
- les mots de passe sont cryptés lorsqu'ils sont transmis de la station de travail au serveur durant l'ouverture de session;
- la sécurité physique du serveur LAN est renforcée en protégeant le serveur dans une salle d'ordinateur spéciale, fermée avec un bloc numérique. De plus, il y a un accès restreint au réseau de la Direction, ce qui assure une double sécurité pour le serveur;
- des sauvegardes complètes pour les serveurs sont effectuées tous les jours et les bandes sont envoyées hors site aux Archives nationales tous les mois;
- l'accès à distance par les télétravailleurs au LAN est bien contrôlé car les mots de passe et les autres contrôles sont utilisés pour se protéger contre un accès non autorisé; et
- l'accès au LAN est protégé grâce à la fonction de « détection d'intrus » de Novell.

Contrôles pour renforcer la sécurité des systèmes

La Direction des corporations peut renforcer la sécurité des systèmes :

- en assurant que le personnel ne puisse pas être branché au LAN à partir de deux stations de travail en même temps;
- en surveillant les alertes d'intrus;
- en réduisant le nombre des tentatives d'ouverture de sessions de relance dans le LAN de cinq à dix-neuf pour une ouverture initiale et pour les nouveaux mots de passe; et
- en protégeant la salle des ordinateurs en changeant le code du bloc numérique tous les 60 jours et en utilisant un mot de passe pour protéger la console de serveur LAN.

Réponse de la gestion

Le gestionnaire, Services informatiques de la Direction des corporations, a accepté les recommandations visant à renforcer la sécurité. Toutes les recommandations ont été mises en oeuvre tel qu'il est indiqué dans le rapport.

Annexe A

Pour fournir une aide supplémentaire à la Direction des corporations, l'Annexe A a été incluses dans le rapport en tant qu'un guide à utiliser lorsque la Direction convertira de NetWare 3.12 à NetWare 4.x.

Contexte

La Direction des corporations d'Industrie Canada administre les lois concernant les entreprises et les entités sans but lucratif qui sont constituées en sociétés sous le régime fédéral. La Direction dispose actuellement d'un serveur Fulcrum Pentium, de deux serveurs 3.12 avec environ 80 utilisateurs réguliers, deux serveurs d'application Siemens, un serveur de développement HP pour un nouveau environnement architectural et un serveur de production HP.

Après la participation de la Direction des corporations à un projet pilote d'un processus d'auto-évaluation de la sécurité des systèmes, la Direction générale de la vérification et de l'évaluation pris les dispositions nécessaires avec la Direction pour vérifier les contrôles de sécurité du réseau local (LAN).

Objectifs

Les objectifs de la présente vérification consistaient à assurer que les contrôles :

- empêchent des modifications non autorisées des données;
- fournissent une base saine pour le contrôle des changements;
- respectent l'exigence opérationnelle à l'effet que toutes les données demeurent intégrales, exactes et valides;
- fournissent un environnement physique sain pour protéger le matériel et les données;
- permettent l'exécution d'importantes fonctions administratives de LAN tous les jours par une série d'activités de soutien;
- fournissent une politique-cadre efficace en matière de sécurité et de contrôle interne;
- fassent en sorte que seuls les personnes autorisées aient accès aux biens liés à la technologie de l'information (y compris les données); et
- fournissent un cadre adéquat pour empêcher et détecter les virus.

Étendue

L'étendue de la vérification a couvert la sécurité de tous les serveurs LAN, de l'accès à distance et des stations de travail situés dans la Direction des corporations. Comme Lotus Notes et l'accès Internet sont administrés centralement, ils ont été exclus da la vérification. Le projet du commerce électronique, élaboré vers la fin de 1997-1998, a également été exclus de la présente vérification.

Méthodologie

Les vérificateurs ont commencé ce projet en se familiarisant avec le LAN et l'environnement de sécurité. Ils ont acquis une connaissance des principaux rôles, responsabilités, mandats et de la mission de la Direction des corporations au sein d'Industrie Canada, ainsi que des politiques et normes pertinentes aux LAN au sein du Ministère.

Une réunion préliminaire s'est tenue entre l'équipe de vérification et le personnel de la Direction pour comprendre l'environnement de la Direction des corporations et se mettre d'accord sur l'étendue et les objectifs de la vérification. On a mené à bien un examen des questionnaires d'auto-évaluation, remplis par le personnel de la Direction des corporations, et des documents sur toutes les politiques et normes pertinentes aux réseaux locaux, y compris Lotus Notes.

On a effectué une évaluation préliminaire du cadre de contrôle de la sécurité en analysant les contrôles pour :

- les opérations LAN, y compris le réseau de communications;
- l'intégrité (exhaustivité, exactitude et autorisation) des données de système et du traitement;
- la disponibilité des données et des services (planification de la contingence et sauvegarde);
- la confidentialité des données (pour se protéger contre une divulgation non autorisée); et
- l'intégrité des données (protection contre la corruption et une modification non autorisée des données).

L'équipe de vérification a élaboré des critères de vérification en utilisant diverses sources, notamment :

- les priorités et les thèmes ministériels;
- les pratiques généralement acceptées dans le secteur privé;
- les lignes directrices normalisées pour la sécurité du LAN;
- les « pratiques exemplaires » utilisées dans l'ensemble de l'industrie privée;
- les autres renseignements pertinents publiés; et
- la vaste expérience des membres de l'équipe de vérification (de Progestic International).

La situation globale a été analysée selon le cadre de vérification évalué pour la sécurité et les critères de vérification mis au point (voir l'Annexe B pour une liste complète des critères de vérification).

Les vérificateurs ont ensuite évalué les questions et les secteurs d'intérêt de la vérification par l'examen des documents, des entrevues avec le personnel, la collecte d'éléments de preuve, l'analyse des renseignements détaillés et la réalisation d'essais de vérification.

On a mené des entrevues avec un échantillon de gestionnaires et utilisateurs qui avaient participé à la conception et à l'installation des LAN (voir Annexe C pour une liste des employés interrogés). On a mené un essai de vérification ainsi que demandé et on a poursuivi le travail sur le terrain en examinant et en évaluant les éléments suivants :

- emplacement des serveurs de fichiers;

- processus de sauvegarde et de récupération, y compris l'utilisation des sources d'alimentation sans coupure (UPS) et le traitement de la sauvegarde automatisée pour les stations de travail et le serveur de fichiers ;
- les procédures d'entretien du matériel;
- l'administration des mots de passe;
- la journalisation et la vérification des activités de sécurité;
- les outils de sécurité utilisés par la Direction des corporations;
- la protection contre les virus;
- les contrôles d'accès à distance;
- les contrôles de la connectivité; et
- les contrôles de l'accès générique à Internet.

Une séance d'information sur les observations faites durant la vérification a été offerte au personnel de la Direction des corporations avant de préparer le rapport de vérification.

Questions

1.0 *ASSURER QUE LES CONTRÔLES EMPÊCHENT DES MODIFICATIONS NON AUTORISÉES DES DONNÉES.*

1.1 Connexions simultanées

Le personnel peut entrer simultanément dans deux stations de travail LAN en même temps. Les données contenues dans le LAN peuvent être corrompues si la même personne essaie d'accéder à partir de deux différentes sources. De plus, si une personne non autorisée est connectée simultanément à deux machines, alors une des machines est soit inactive, soit utilisée par une personne non autorisée. Si le nom de compte et le mot de passe d'utilisateur sontt découverts dans la station de travail inactive, la Direction court le risque qu'un individu non autorisé accède au LAN. L'individu autorisé serait ensuite responsable des actions de la personne non autorisée.

Recommandation

Il faut interdire à chaque utilisateur de LAN d'entrer simultanément dans deux stations de travail. Pour ce faire, on pourrait établir le « paramètre des connexions simultanées » à « 1 ». Grâce à la mise en oeuvre de cette recommandation, on ne place aucuns frais généraux supplémentaires sur le LAN, et on n'engage aucun coût en changeant ce paramètre.

Réponse de la gestion

Cette recommandation a été mise en oeuvre.

2.0 *ASSURER QUE LES CONTRÔLES FOURNISSENT UNE BASE SAINE POUR LE CONTRÔLE DES CHANGEMENTS.*

2.1 Correcteurs Novell

Les correcteurs représentent une réparation ou une modification apportée au système d'exploitation Novell (NetWare). Parfois, les corrections sont installées pour accroître le rendement et la fonctionnalité de NetWare.

Dans le cadre de l'essai de vérification, les vérificateurs ont examiné la liste des correcteurs installés dans le serveur LAN et les stations de travail. Les vérificateurs ont constaté que le plus récent correcteur pour l'authentification des clients n'est pas la récente version du Virtual Loadable Module (VLM). La version VLM trouvée était la version 1.20 (941108). Novell a confirmé que la plus récente version du VLM est la version 1.21. Bien que la Direction des corporations ne connaisse aucun menace à l'intégrité de ses données de LAN, la version 1.20 du VLM, au lieu de la version 1.21, pourrait causer une augmentation dans les frais généraux administratifs et une plus grande possibilité de problèmes pour les administrateurs du LAN.

Le correcteur LIBUPC.EXE, le correcteur STRTL5.EXE et le correcteur VRPUPI.EXE sont les plus récentes versions dans le serveur LAN. La date du correcteur SMSUP.EXEdans le serveur LAN est le 1er mars 1996. Le plus récent correcteur devrait être daté du 23 juillet 1996.

Bien que seulement deux correcteurs ne soient pas récents, le fait de ne pas mettre à jour les correcteurs Novell expose la Direction au risque des fonctions LAN sujettes à l'erreur et au risque de ne pas avoir une fonctionnalité offerte par Novell.

Recommandation

La Direction des corporations devrait installer toutes les versions actuelles des correcteurs sur une base opportune. Pour gérer ce processus, la Direction devrait établir un journal qui documente les éléments suivants :

- les correcteurs de dates sont reçus de Novell et installés
- les raisons d'avoir installé le correcteur et la justification de ne pas en avoir installé un; et
- la signature de l'administrateur LAN.

Réponse de la gestion

Cette recommandation a été mise en oeuvre.

3.0 *ASSURER QUE LES CONTRÔLES RESPECTENT L'EXIGENCE OPÉRATIONNELLE À L'EFFET QUE TOUTES LES DONNÉES DEMEURENT INTÉGRALES, EXACTES ET VALIDES.*

3.1 Traitement et les journaux de détection d'intrus

Le journal d'erreur du serveur LAN et le fichier journal de console sont produits automatiquement par le système d'exploitation Novell. Ces journaux contiennent des renseignements importants, notamment : le compte, la date et le temps d'accès, les fichiers accédés, les applications utilisées, les erreurs, le temps de fermeture de session et d'autres renseignements importants. Par exemple, le fichier SYSSLOG.ERR avise les administrateurs LAN des intrus qui essaient d'accéder au réseau. Le fichier CONLOG.TXT capte les commandes utilisées dans le serveur. Il est important d'examiner ce fichier pour vérifier les commandes qui sont émises à la console et, probablement, prévoir les menaces à l'environnement LAN.

Le journal de détection d'intrus est également configuré pour bloquer un compte valide si un mot de passe invalide est utilisé après un nombre prédéterminé de tentatives consécutives. Après l'écoulement du temps expiré, l'utilisateur peut entrer dans le réseau encore une fois.

Une méthode utilisée par les personnes qui essaient d'accéder à un LAN est d'utiliser un mot perceur de mot de passe. Ce logiciel essaie de deviner les mots de passe des utilisateurs en lisant le fichier de mot de passe situé dans le serveur de fichier Novell. Les vérificateurs ont essayé d'utiliser un perceur de mot de passe pour assurer

que les mots de passe sont difficiles à deviner. Comme la détection d'intrus est invoquée, le perceur de mot de passe ne pouvait pas fonctionner. Il s'agit d'un contrôle préventif efficace.

Les vérificateurs ont constaté que ces journaux n'étaient pas surveillés régulièrement. Cela expose la Direction au risque de ne pas pouvoir détecter les accès non autorisés, les problèmes ou les modèles d'usage. Les vérificateurs ont examiné le fichier journal d'erreur de la console et ont découvert que deux verrouillages d'intrus étaient actifs. Si l'administrateur de LAN examinait le même fichier journal, il aurait pu étudier la cause des verrouillages.

Recommandation

La Direction des corporations devrait établir une politique qui énonce que l'administrateur de LAN examinera régulièrement les journaux, documentera toutes constatations observées et cherchera des procédures préventives lorsque les erreurs sont de nature importante.

Réponse de la gestion

La Direction a mis en oeuvre cette recommandation. Elle documentera les dates auxquelles ces journaux ont été surveillés. En plus de mettre en oeuvre cette recommandation, la Direction des corporations a installé un analyseur de LAN pour surveiller l'efficacité du réseau.

3.2 Fermeture de session automatique / Économiseur d'écran

Lorsque les utilisateurs laissent leurs stations de travail sans surveillance pour une période de temps, un contrôle efficace causerait la station de travail de fermer la session LAN automatiquement afin de minimiser le risque d'un accès non autorisé à la station de travail inactive. Or, ce contrôle n'est pas utilisé dans de nombreux cas car il n'est pas considéré pratique.

Toutefois, un logiciel d'économiseur d'écran avec un mot de passe est un contrôle de rechange à la fermeture de session automatique. L'utilisation d'un logiciel d'économiseur d'écran réduit également l'usure de l'écran et, si un mot de passe est utilisé, empêche une utilisation non autorisée de la station de travail. Quelques stations de travail ont été sélectionnées pour mettre à l'essai ce contrôle. D'après les résultats de l'essai, un économiseur d'écran avec mot de passe n'était pas utilisé. Selon l'administrateur de LAN, seuls 40 p. 100 des utilisateur sont mis en marche leurs économiseurs d'écran.

Pour utiliser efficacement l'économiseur d'écran avec un mot de passe, il faut établir une limite de temps après quoi l'économiseur d'écran se met en marché automatique. Si le délai est trop long, les avantages de l'économiseur d'écran avec un mot de passe sont perdus car la station de travail sera toujours exposée à un accès non autorisé. Pour utiliser ce contrôle de façon pratique, on peut établir une limite de temps plus longue et montrer à l'utilisateur comment activer l'économiseur d'écran en cas d'une longue absence prévue de la station de travail.

Comme la Direction travaille derrière des portes sécuritaires, le risque qu'une personne puisse accéder est minime si ce contrôle n'est pas utilisé.

Recommandation

Bien que la Direction fonctionne derrière des portes sécuritaires, la Direction des corporations devrait encourager les utilisateurs à mettre en marché un économiseur d'écran avec un mot de passe afin de renforcer la protection contre les accès non autorisés. Pour faciliter l'utilisation du contrôle, l'administrateur de LAN devrait conseiller les utilisateurs sur la limite de temps appropriée et sur la façon d'activer le verrouillage de l'économiseur d'écran lorsque l'utilisateur le souhaite.

Un essai périodiq de contrôle par la sélection d'un échantillon de stations de travail au hasard vérifierait à quel point les utilisateurs s'adaptent à ce contrôle.

Réponse de la gestion

Cette recommandation a été acceptée par la Direction. L'administrateur de LAN encouragera l'utilisation d'un économiseur d'écran avec un mot de passe et mettra à l'essai ce contrôle régulièrement.

4.0 *ASSURER QUE LES CONTRÔLES FOURNISSENT UN ENVIRONNEMENT PHYSIQUE SAIN POUR PROTÉGER LE MATÉRIEL ET LES DONNÉES.*

4.1 Accès

L'accès à la salle des ordinateurs est contrôlé par une porte verrouillée qui dispose d'un accès à bloc numérique. Seuls les employés qui ont besoin d'un accès connaissent le code du bloc numérique. De plus, le personnel d'entretien est supervisé en tout temps lorsqu'il doit accéder à la salle des ordinateurs.

Le code d'accès numérique est changé uniquement lorsqu'un membre de personnel quitte. Le changement infréquent du code d'accès du bloc numérique expose la Direction à l'accès de personnes non autorisées à la salle des ordinateurs.

Pour une protection plus poussée, la console du serveur LAN peut être protégée par un mot de passe afin de restreindre l'accès. Ce contrôle n'était pas utilisé. Le changement infréquent du code d'accès numérique, conjugué à une console de serveur non bloqué, expose la Direction des corporations à un risque plus grand d'accès non autorisé.

Recommandation

La Direction des corporations devrait changer le code d'accès numérique au moins une fois tous les 60 jours, ou plus tôt, si un employé quitte la Direction. La Direction devrait aussi veiller à ce que le console de serveur LAN soit protégé par un mot de passe en tout temps.

Réponse de la gestion

Cette recommandation a été mise en oeuvre. À l'avenir, la Direction des corporations enregistrera, dans le journal d'exploitation imprimé, la date à laquelle le code d'accès numérique et la console du serveur LAN sont changés. Cela sera effectué une fois tous les 60 jours, ou plus tôt, si un employé quitte la Direction.

4.2 Alimentation électrique

La Direction des corporations a branché les serveurs LAN à un système d'alimentation sans coupure (UPS). Cela permettra aux serveurs de fonctionner pendant environ cinq minutes en cas d'une panne d'électricité. Les vérificateurs croient que cinq minutes ne sont pas suffisants pour bien fermer le serveur de fichier.

Recommandation

Le système UPS devrait accorder aux serveurs un temps minimal de 20 minutes d'opération en cas d'une panne d'électricité.

Réponse de la gestion

L'administrateur LAN a mis à l'essai le délai de cinq minutes et a trouvé qu'une fermeture ordonnée était possible. Toutefois, la Direction des corporations convient qu'une limite de temps plus longue serait préférable. Elle cherchera donc à changer la limite de temps.

5.0 *ASSURER QUE LES CONTRÔLES PERMETTRONT L'EXÉCUTION D'IMPORTANTES FONCTIONS ADMINISTRATIVES DE LAN PAR UNE SÉRIE D'ACTIVITÉS DE SOUTIEN.*

5.1 Traitement de sauvegarde

Les sauvegardes complètes du serveur sont effectuées tous les jours, du lundi au vendredi. Après chaque sauvegarde, la personne qui exécute la sauvegarde signe le journal des sauvegardes. Les bandes sauvegardées sont conservées hors site aux Archives nationales tous les mois.

D'après l'examen des journaux de sauvegarde, on a constaté que les sauvegardes avaient été signées avec succès dans le journal des sauvegardes au cours des trois derniers mois. Les vérificateurs ont notés qu'il existe quatre bandes de sauvegardes quotidiennes et une bande hebdomadaire. Ces bandes étaient clairement étiquetées.

Le personnel est encouragé à placer toutes ses données sur l'unité « P: » du LAN. Cela assure que les données sont sauvegardées régulièrement dans le cadre d'un processus de sauvegarde normal du LAN. Toutefois, on a trouvé que certains individus sauvegardent leurs données dans leur disque dur local (l'unité « C: »). Il n'y a aucune preuve que ces individus font des copies de secours de leurs données enregistrées sur le réseau local.

Recommandation

La Direction des corporations devrait rappeler au personnel que les données sur l'unité « C » de leur disque dur local n'est pas toujours sauvegardé par l'administrateur de LAN.

Réponse de la gestion

La Direction des corporations prévoit envoyer des rappels trimestriels sur les questions en matière de sécurité, par exemple rappeler au personnel que l'administrateur de LAN n'effectue aucune sauvegarde sur l'unité « C » afin d'encourager le personnel à sauvegarder les données sur l'unité « P » du serveur.

5.2 Mise à jour des mots de passe

La politique de la Direction des corporations énonce que les mots de passe doivent être changés tous les 90 jours. Cela constitue une bonne pratique pour les utilisateurs. Cependant, on a découvert que le mot de passe du superviseur de LAN est changé uniquement lorsqu'un employé ou un conseiller quitte la Direction. Selon nous, cela est insuffisant et expose la Direction des corporations à un plus grand risque que des personnes non autorisées découvrent le mot de passe du superviseur.

Recommandation

La Direction des corporations devrait mettre en oeuvre une politique qui exige que le mot de passe du superviseur soit changé au moins une fois tous les 30 jours.

Réponse de la gestion

La Direction des corporations a mis en oeuvre cette recommandation.

6.0 *ASSURER QUE LES CONTRÔLES FOURNISSENT UNE POLITIQUE-CADRE EFFICACE EN MATIÈRE DE SÉCURITÉ ET DE CONTRÔLE INTERNE.*

6.1 Utilitaires Novell NetWare

Les utilitaires NetWare, tels que SYSCON, NETCON, RCONSOLE, sont en mode lecture seulement afin de les protéger d'une modification ou d'une suppression accidentelles.

Les fichiers de configuration de clients NetWare situés au niveau des stations de travail individuelles (comme Net.cfg et Startnet.bat) ne sont pas protégés et peuvent être accidentellement effacés. Si ces fichiers sont accidentellement modifiés ou effacés, alors la Direction des corporations est exposée au risque de voir les utilisateurs perdre leur connectivité LAN. L'administrateur LAN doit alors reconnecter l'utilisateur. De plus, si un utilisateur perd sa connectivité pendant qu'il modifie des données, les données pourraient alors être corrompues.

Recommandation

La Direction des corporations devrait assurer que les fichiers clients de NetWare sont protégés contre une modification accidentelle.

Réponse de la gestion

L'administrateur de LAN a changé ces fichiers en mode de lecteur seulement dans toutes les stations de travail. En outre, les copies de ces fichiers pour chaque utilisateur se trouvent désormais dans un nouveau répertoire sur le serveur LAN. Cela sert d'une mesure de secours pour assurer que si un utilisateur efface accidentellement ses fichiers, l'administrateur LAN peut copier les fichiers à partir du serveur LAN dans la station de travail de l'utilisateur.

7.0 *ASSURER QUE LES CONTRÔLES FASSENT EN SORTE QUE SEULES LES PERSONNES AUTORISÉES AIENT ACCÈS AUX BIENS LIÉS À LA TECHNOLOGIE DE L'INFORMATION (Y COMPRIS LES DONNÉES).*

7.1 Ouverture de session

Les scripts essentiels d'ouverture de session LAN, comme NETSSYS.DAT, sont protégés. Les utilisateurs peuvent visualiser les scripts d'ouverture de session, mais ne peuvent pas les modifier, les supprimer ou les renommer. Ils sont protégés contre une modification ou une suppression accidentelles.

7.2 Accès à distance

Les utilisateurs ont la capacité de composer à distance dans le LAN pour accéder au courrier et aux ressources du réseau. Des contrôles efficaces de logiciel d'accès à distance (ReachOut) sont utilisés. L'utilisateur entre un mot de passe et le logiciel d'accès à distance compose un numéro préétabli. Lorsque l'utilisateur appelle à partir d'un tableau de distribution, une carte de sécurité avec un numéro passe est synchronisée ou associée avec le numéro de code donné par l'utilisateur. Il s'agit de contrôles efficaces.

La commande RCONSOLE permet à l'utilisateur d'accéder à la console du serveur LAN de Novell à partir d'une station de travail branchée au réseau. Si on permet l'exécution de cette commande par tout le monde, l'environnement LAN court le risque que des personnes non autorisées exécutent les commandes de console. La

Direction des corporations a protégé la commande RCONSOLE par un mot de passe et les utilisateurs réguliers n'ont pas accès à cette commande. Cela représente un contrôle solide.

7.3 Récupération des fichiers supprimés

Lorsque les fichiers sont effacés, ils ne sont pas supprimés de façon définitive car ils restent sur le disque dur. Seules les entrées de répertoire sont effacées. DOS permet à personnes de récupérer des fichiers si ces derniers ont été supprimés accidentellement. Néanmoins, la commande UNDELETE n'est pas permise par Novell.

Novell fonctionne de la même manière que DOS. Les fichiers supprimés sont retenus jusqu'à ce que l'espace disque qu'ils occupent soit réutilisé. Toutefois, Novell ne permet pas l'utilisation de la commande UNDELETE; au lieu de cela, il dispose d'une commande appelée « salvage » (« récupération »). Il s'agit d'une commande utile pour les administrateurs de LAN pour récupérer les fichiers effacés accidentellement. Les utilisateurs peuvent récupérer uniquement les fichiers auxquels ils ont un accès de création.

7.4 Inventaire

On a comparé le rapport d'inventaire de la Direction des corporations avec le rapport de l'inventaire général d'Industrie Canada. Aucun écart n'a été décelé. De plus, les vérificateurs ont été en mesure de localiser physiquement tout le matériel énuméré dans les deux rapports d'inventaire.

7.5 Ouvertures de session de relance

Les ouvertures de session de relance désignent le paramètre de NetWare qui fournit à une personne la capacité d'entrer dans le LAN un certain nombre de fois avec un mot de passe périmé. Cela est utilisé principalement lorsque les mots de passe sont automatiquement changés et aussi pour les nouveaux utilisateurs.

On a constaté que les ouvertures de session de relance pour une ouverture initiale ou les nouveaux mots de passe dans le LAN est une série de 19 tentatives. Cela signifie qu'une personne a 19 tentatives pour accéder au LAN. Dans le cas d'un changement automatique d'un mot de passe, cela peut s'élever à plusieurs semaines.

Recommandation

Ce paramètre devrait être changé à un maximum de cinq ouvertures de session de relance pour une plus grande protection.

Réponse de la gestion

Ce paramètre a été changé à cinq tel qu'il est recommandé.

7.6 Droits d'accès

Les utilisateurs jouissent actuellement de pleins droits, sauf les droits « S » des superviseurs, à leur répertoire et fichiers personnels. Cela signifie qu'ils ont le pouvoir de lire, d'écrire, de créer, d'effacer, de modifier, de balayer et de fournir un contrôle d'accès (à leurs fichiers) aux autres utilisateurs.

Le fait d'avoir un droit d'« accès » permet à un utilisateur de donner aux autres utilisateurs le droit d'accéder à ses fichiers et répertoires personnels ou de modifier les droits d'héritage des fichiers et des répertoires. En d'autres mots, l'utilisateur devient un mini-superviseur. Par exemple, Jean a les droits « A » à son répertoire personnel et peut accorder le plein droit à Pierre. Pierre peut alors modifier et supprimer les fichiers de Jean.

Bien que la plupart des utilisateurs au sein de la Direction des corporations ne sachent pas comment exécuter la fonction, le fait de concéder des droits expose quand même la Direction des corporations au risque que des personnes non autorisées puissent accéder aux fichiers LAN.

Recommandation

La Direction des corporations ne doit pas permettre aux utilisateurs réguliers d'avoir un droit d'accès « A » à leurs répertoires personnels.

Réponse de la gestion

Cette recommandation a été mise en oeuvre.

8.0 *ASSURER QUE LES CONTRÔLES FOURNISSENT UN CADRE ADÉQUAT POUR EMPÊCHER ET DÉTECTER LES VIRUS.*

Il existe actuellement plus de 6 000 virus connus : trois nouveaux virus sont découverts chaque jour. Afin de minimiser la possibilité d'une attaque de virus, la Direction des corporations s'adhère à la politique d'Industrie Canada sur les virus dans le « *ISTC Handbook on IT Security For Shared-Facility (LAN) & Application Managers* ». Cette politique indique que les utilisateurs doivent être ordonnés à exécuter systématiquement des programmes recommandés et mis à jour de balayage antivirus. La Direction vérifie régulièrement ses disques durs au moyen du logiciel Norton Anti-Virus (NAV). Il s'agit d'un contrôle solide.

Les renseignements relatifs aux virus qui ont été détectés sont placés dans la base de connaissances de Lotus Notes. Cela permet à la Direction de surveiller les renseignements statistiques concernant les virus détectés et la rechercher sur les virus détectés.

8.1 Virus Internet

Les fichiers téléchargés du World Wide Web par Internet ou des pièces jointes dans les courriels en provenance d'Internet doivent être balayés par chaque employé avant d'exécuter le fichier ou de le lire. L'utilitaire Norton Anti-Virus utilisé chez Industrie Canada effectue cela automatiquement. NAV balaie automatiquement les fichiers avant qu'ils ne soient ouverts.

Dans la plupart des cas, la procédure susmentionnée est adéquate. Toutefois, dans certains cas, un virus peut s'échapper. Industrie Canada, tout comme les nombreux autres ministères du gouvernement, ne dispose pas d'un processus pour balayer automatiquement les fichiers avant que ces derniers se rendent aux stations de travail individuelles.

Le produit *Norton AntiVirus for Internet E-mail Gateways* effectue une recherche de virus dans les fichiers afin de détecter les virus avant qu'ils ne se rendent aux stations de travail individuelles. Ce produit balaie automatiquement les fichiers sur la passerelle du protocole de transfert de courrier simple (SMTP). Il intercepte et détruit automatiquement tout virus pouvant être caché dans des pièces jointes à un courriel avant que les virus ne causent des dommages ou avant qu'ils ne se répandent.

Cela n'a pratiquement aucun impact sur le rendement du réseau ou du pare-feu. Ce produit est transparent aux utilisateurs et arrête les virus avant qu'ils puissent atteindre les stations de travail individuelles. Il avise même l'émetteur et la réception du courriel qu'un virus a été détecté.

On peut télécharger l'outil *Norton AntiVirus for Internet E-mail Gateways* à partir du site Web de Symantec pour une période d'essai de gratuite de 30 jours.

Recommandation

Comme la passerelle SMTP ne relève pas de la responsabilité de la Direction des corporations, la Direction générale de la vérification et de l'évaluation fera part de cette recommandation aux personnes responsables de la passerelle.

Réponse de la gestion

Pour renforcer ce contrôle davantage, la Direction des corporations ajoutera une colonne dans le « journal » pour indiquer la date à laquelle l'Administration LAN a installé la version mise à jour du logiciel NAV sur le réseau de la Direction.

ANNEXE A

GUIDE À UTILISER LORSQUE LA DIRECTION CONVERTIRA DE NetWare 3.12 à NetWare 4.x.

La présente Annexe est destinée à l'usage du personnel technique. Elle décrit les différences entre NetWare 3.12 et NetWare 4.x Elle comprend les préparatifs pour la migration et les différences des méthodes de migration et des fonctions de sécurité.

Voici un résumé des différences entre NetWare 3.12 et NetWare 4.x:

- facilité d'administration, avec plus d'utilitaires NetWare améliorés (NetWare Professional Reference - 4e édition, Karanjit Siyan, PhD - New Riders Publishing, 1995 p. 345);
- Services de répertoire NetWare (NDS). Les utilisateurs entrent désormais dans les NDS (NetWare Directory Services) qui authentifient tous les serveurs sur le réseau;
- amélioration dans la gestion du système de fichiers NetWare;
- sécurité et gestion améliorées du système de fichiers;
- soutien à la vérification du réseau;
- architecture de gestion de mémoire simplifiée et plus efficace;
- niveaux plus élevés d'utilisation de disque et maximisation en raison d'une attribution de sous-blocs et d'une compression de fichiers; et
- niveaux plus élevés de tolérance aux failles avec System Fault Tolerance niveau III (SFT III) où il peut y avoir tout point de défaillance unique.

Préparatifs préliminaires

Exécution de bindfix et vrepai

Ce sont des utilitaires fournis par Novell pour corriger les fichiers corrompus, la base de données Bindery et les questions relatives au matériel. Ces utilitaires assurent l'intégrité des fichiers Bindery et suppriment les répertoires de courrier et les droits de fiducie de tous les utilisateurs qui n'existent plus sur le serveur.

Nettoyage du système de fichiers

Balayer les répertoires sur le serveur et supprimer les fichiers et les répertoires qui ne sont plus nécessaires. Le programme d'installation de la stratégie de migration sur place a besoin d'un espace de disque libre d'environ 50 megabytes dans le volume SYS. Par conséquent, exécuter la fonction de purge de NetWare pour nettoyer les fichiers inutiles et aider à libérer des blocs en suspens.

Avant d'entamer la migration, faire des copies de secours de STARTUP.NCF et AUTOEXEC.NCF. Pour les besoins de sauvegarde, imprimer un exemplaire du script d'ouverture de session du système, intitulé NETSLOG.DAT dans le répertoire SYS:PUBLIC.

Essai

Tester les Virtual Loadable Modules (VLM) et les fichiers d'authentification des clients, comme « net.cfg » et « startnet.bat ». « Net.cfg » est un fichier de configuration qui contient tous les cadres non établis par défaut pour l'environnement de la Direction des corporations environnement. Communiquer avec tous les vendeurs de logiciels pour obtenir l'assurance que leurs applications fonctionneront avec VLM.

Appellation ***conventionnelle***

Les appellations conventionnelles représentent une série de règles qui régissent la façon dont les objets seront définis sur le réseau. NetWare 4.x vous permet d'avoir de noms d'objet complet d'une longueur maximale de 255 caractères. En établissent les appellations conventionnelles, vous pouvez assurer une uniformité et une facilité d'utilisation des noms affectés et ce, dans l'ensemble du réseau. Les appellations conventionnelles couvrent des objets, tels que noms d'utilisateur, les noms de serveur et les imprimantes. Les appellations conventionnelles doivent être établies avant la migration à NetWare 4.x, car il sera impossible d'effectuer des changements après la mise en oeuvre. Voici quelques-unes des suggestions générales pour les appellations conventionnelles :

- garder le nom court et descripteur;
- être uniforme dans l'ensemble du réseau; et
- utiliser des caractères alpha-numériques, dans la mesure du possible.

Arbre

Étant donné que NetWare 4.x authentifie les utilisateurs dans un arbre et non un serveur, l'élaboration de normes d'appellation est très importante. NetWare 4.x utilise l'arbre Network Directory Structure (NDS) pour définir tous les objets. La NDS est appelée arbre car elle est logiquement définie de la même manière qu'un arbre à l'envers. Lorsque vous installez le serveur NetWare 4.x, vous nommerez l'arbre et définirez le contexte (ou l'emplacement dans l'arbre) dans lequel l'objet serveur résidera.

Sauvegarde

Assurer qu'une sauvegarde pleinement réussie a été menée à bien avant d'exécuter la mise à niveau.

Désactiver les ouvertures de sessions et fermer les passerelles de courriel, les virus, Internet, Lotus Notes qui fonctionnent sur le serveur. Il est important de fermer tout ce qui garde les fichiers ouverts sur le serveur. Cela assure qu'aucun fichier n'est omis durant la sauvegarde.

Méthodes de migration

Il existe trois façons de migrer au NetWare 4.X:

1. Mise à niveau sur place

Cette méthode utilise le programme d'installation (« install.nlm ») pour installer la version de NetWare directement sur votre serveur 3.12 existant. Tous les renseignements Bindery et les renseignements sur le système de fichiers sont mis à niveau sur place dans votre serveur existant.

Le désavantage de cette méthode survient en cas d'un problème. Vous devez alors retourner à votre version précédente de NetWare. Vous devez remettre à l'état initial la sauvegarde faite antérieurement avant d'installer la version NetWare 4.X. Le retour à la version précédente de NetWare peut s'avérer très fastidieux.

L'avantage de cette méthode est le fait qu'une machine serveur est nécessaire et que les mots de passe des utilisateurs sont retenus. Cette méthode n'est pas recommandée à cause des nombreux désavantages.

2. Méthode d'un fil à l'autre

Pour cette méthode, vous devez établir un nouveau serveur NetWare 4.1 en utilisant un nouveau matériel, alors que l'ancien serveur continue de fonctionner. Par conséquent, vous avez besoin d'un serveur source et d'un

serveur de destination. Les renseignements du serveur 3.12 existant est migré au nouveau serveur au moyen de « dsmigrate » et les utilitaires de migration de fichiers fonctionnent à partir d'une station de travail attachée aux deux serveurs. Il s'agit de la méthode la plus sécuritaire, sauf qu'elle exige une pièce supplémentaire de matériel.

Les renseignements Bindery sont les premiers à être déplacés au répertoire de travail sur la station de travail qui exécute l'utilitaire MIGRATE, traduit au format NetWare 4.x. et puis transférés au serveur de destination. Cette méthode de migration vous permet de préserver l'environnement du serveur initial. Il y a un risque minimal de perte de données durant le processus de migration.

Étapes pour la migration « d'un fil à l'autre » :

A. Planifiez votre arbre NDS. (Nota : vous n'êtes pas obligé de planifier votre arbre au complet à ce stade-ci; planifiez seulement la structure.)

B. Installez NetWare 4.x sur le nouveau serveur

C. Entrez dans vos serveurs de destination et de source. Avant d'exécuter la migration DS et la migration fichiers, vous devez être lié aux serveurs appropriés. À partir d'une station de travail, entrer en tant qu'administrateur dans le nouvel arbre NDS qui contient votre serveur de destination, puis sélectionnez cet arbre comme votre arbre de choix.

.D. Commencez la migration DS et exécutez l'option de découverte. Commencez l'utilitaire NWADMIN et sélectionnez « DS Migrate » de la barre d'outils.

E. Modelez l'arbre hors ligne.

F. Configurez l'arbre NDS en direct.

G. Commencez l'utilitaire de migration de fichiers.

H. Sélectionnez un volume de source.

I. Sélectionnez le répertoire de destination.

J. Migrez les données du système de fichiers.

Nota :

Une fois que la sauvegarde est terminée, assurez que les plus récents correcteurs sont appliqués.

Bien que la répartition de sous-blocs et la compression de fichiers soient permises par défaut, assurez que cela a été bel et bien exécuté. On peut vérifier cela en utilisant l'utilitaire SERVMAN de NetWare. Cela maximisera l'utilisation de disque.

3. Méthode du même serveur

Cette méthode déplace toutes les données hors ligne, met à niveau le système d'exploitation et le matériel du serveur, puis migre les données au même serveur. Cela est utilisé au moment de mettre à niveau un serveur qui sera installé dans le même matériel que l'ancien serveur source. Même si vous utilisez uniquement un seul serveur avec cette méthode, certains risques entrent en jeu. De plus, vous pourriez ne pas être en mesure de migrer les attributs de fichiers et les droits de fiducie. Si, pour une raison quelconque, le processus de migration connaît une faille, vous pourrez ne pas disposer d'un serveur auquel se fier et vous devrez réinstaller le système d'exploitation de départ et remettre la bande à l'état initial. Vous devrez recourir à un programme de sauvegarde

d'un tiers au moment d'exécuter ce processus car les outils de sauvegarde NetWare ne sont pas appuyés par cet utilitaire de migration.

Pour accomplir cette méthode, vous devez d'abord sauvegarder les fichiers de données sur une unité de bande et migrer les renseignements Bindery au répertoire de travail dans la station de travail. Vous installez ensuite NetWare 4.x dans votre serveur initial. Enfin, vous restaurez les données de la bande et traduisez et migrez les renseignements Bindery de la station de travail au nouveau serveur NetWare 4.x

Questions en matière de sécurité

- NetWare 4.x ajoute un composant supplémentaire nommé Network Directory Services (NDS). Les trois éléments de la sécurité NetWare 4.x sont : la sécurité d'ouverture de session, la sécurité NDS et la sécurité du système de fichier.

  1. Sécurité d'ouverture de session - Cela contrôle les personnes qui peuvent obtenir une entrée initiale dans le réseau. L'authentification de l'ouverture de session d'un utilisateur doit être réalisée par rapport à l'objet enregistré dans la base de données générale NDS. Les restrictions d'ouverture de session visent des objets NDS, notamment : les restrictions de comptes, les restrictions de mots de passe, de restrictions de stations, les restrictions de temps, et les limites d'intrus.
  2. Sécurité NDS - Cet élément est utilisé pour déterminer à quelles ressources du réseau (objets NDS) l'utilisateur a le droit d'accéder. Le terme « droits » désigne le genre d'opérations qu'un utilisateur peut exécuter sur un objet NDS.
  3. Sécurité du système de fichiers - Cet élément est très similaire à la sécurité NDS. Cela s'applique aux fichiers et aux répertoires à l'extérieur du répertoire personnel de l'utilisateur.

- NDS - Sachez que les utilitaires tels que NWADMIN sont très puissants et doivent avoir un accès limité. Il faudrait envisager d'enlever cet utilitaire de l'accès général et de le placer dans un répertoire séparé avec seulement un accès d'administrateur.
- Assurez qu'une stratégie est mise en oeuvre pour concéder les droits sous forme d'affectations de groupes.
- Songez à déplacer d'autres utilitaires de NetWare, tels que NETADMIN et RCONSOLE dans des répertoires séparés avec NWADMIN.
- Envisagez la possibilité de créer des IRF (filtres de droits d'héritage) pour bloquer les droits au NetWare SYS:SYSTEM.
- Créez des comptes pour les administrateurs avec un droit « S » autre qu'ADMIN (défaut), évitez les comptes génériques ayant le droit « S » à cause du manque de responsabilisation.
- Une nouvelle caractéristique de NetWare 4.X est la fonction « AUDITCON » qui permet aux vérificateurs de tracer les étapes des utilisateurs et/ou des administrateurs. En d'autres termes, AUDITCON vous permettra de voir les fichiers et les répertoires qu'un individu a visualisés.
- NetWare 4.X fournit le plus haut niveau de tolérance aux failles (SFT III). Il s'agit d'un miroir complet du serveur intégral. Par conséquent, si un composant du serveur de production accuse d'une faille, le serveur de secours peut prendre la relève, sans que les utilisateurs connaissent un temps d'indisponibilité.

- Cryptage des mots de passe - Lorsque les utilisateurs entrent dans la version 3.0 ou les versions ultérieures de Netware, leur mot de passe est crypté avant d'être envoyé à travers le réseau. Cela empêche que les pirates informatiques déchiffrent le mot de passe en utilisant un analyseur de protocole ou tout autre dispositif qui interrompt les paquets de réseau.

  Toutefois, le cryptage peut causer des problèmes s'il y a des serveurs qui utilisent les services antérieurs à 3.0 de Netware. Par conséquent, Netware 4.x permet au gestionnaire de changer le défaut et de décrypter les mots de passe. Pour ce faire, on peut utiliser l'utilitaire SERVMAN qui offre un moyen de changer les paramètres de démarrage du serveur, y compris le cryptage des mots de passe. Netware 4.x désactive par défaut le paramètre « Allow Unencrypted Passwords », ce qui signifie que les mots de passe sont cryptés.

  En plus d'utiliser des mots de passe comme première ligne de défense, Netware 4.x fournit des fonctions améliorées de sécurité. Une de ces fonctions est l'authentification visant à vérifier si les utilisateurs sont autorisés à utiliser le NDS. Cela est désigné sous le nom de sécurité basée sur le réseau. L'authentification assigne une identification unique à chaque utilisateur pour chaque session d'ouverture. C'est l'identification, et non le mot de passe de l'utilisateur, qui sert à authentifier les demandes d'accès au réseau de chaque utilisateur. La sécurité est améliorée car le mot de passe n'est jamais transmis dans l'ensemble du réseau où il pourrait être surveillé. Il n'est transmis qu'au serveur. L'authentification garantit que le mot de passe de l'utilisateur ne s'étend pas au-delà du processus d'ouverture de session.

ANNEXE B

CRITÈRES DE VÉRIFICATION

Les critères de vérification suivants ont été utilisés pour déterminer l'efficacité des contrôles :

SÉCURITÉ

1. L'accès logique au LAN et l'utilisation du LAN devraient être restreints par la mise en oeuvre de mécanismes d'authentification adéquats relatifs aux règles d'accès.
2. Des procédures devraient être mises en oeuvre pour se conformer à la politique sur la sécurité qui prévoit un contrôle de sécurité d'accès selon le besoin démontré des individus à visualiser, ajouter, changer ou supprimer des données.
3. Des procédures devraient être mises en place pour assurer une action opportune relative à la demande, à l'établissement, à l'émission et à la fermeture de comptes.
4. Un processus de contrôle devrait être mis en place pour examiner et confirmer périodiquement les droits d'accès.
5. Des contrôles devraient être place pour assurer que l'identification et les droits d'accès des utilisateurs, ainsi que l'identité de la propriété du système et des données sont établis et gérés d'une manière centrale pour obtenir un contrôle d'accès global.
6. L'administration de sécurité de la Direction des corporations devrait assurer que les activités de violation et de sécurité sont ouvertes, déclarées, examinées et échelonnées de manière appropriée et régulière afin d'identifier et de résoudre les incidents relatifs à une activité non autorisée.
7. Une capacité de traitement d'un incident de sécurité informatique devrait exister pour aborder les incidents en matière de sécurité. Il faudrait établir des responsabilités et des procédures de gestion des incidents afin d'assurer une intervention appropriée, efficace et ordonnée aux incidents sécuritaires.
8. La gestion devrait établir un bon cadre de mesures de contrôle préventives et détectrices.
9. Tout le personnel devrait être formé et sensibilisé aux principes de sécurité de système. Le programme de formation devrait inclure les aspects suivants : la conduite éthique de la fonction des services d'information, les pratiques de sécurité pour se protéger contre les dangers des défaillances qui nuisent à la disponibilité, à la confidentialité, l'intégrité et au rendement des tâches d'une manière sécuritaire.

GESTION

10. La gestion devrait définir et mettre en oeuvre un système de gestion des problèmes pour assurer que tous les événements qui ne font pas partie d'une opération type (incidents, problèmes et erreurs) sont enregistrés, analysés et réglés au moment opportun. Des rapports d'incidents devraient être établis en cas de problèmes significatifs.
11. La gestion devrait assurer qu'il existe une protection adéquate des renseignements délicats durant la transmission et le transport contre une modification ou un accès non autorisés.
12. La gestion devrait mettre en oeuvre des procédures pour assurer la non-divulgation des renseignements de nature délicate. Les procédures devraient garantir que les données médiatiques marquées aux fins de disposition sont examinées et traitées en conséquence pour éviter que les données délicates soient extraites par un tiers d'un média disposé.

MÉDIA

13. Des procédures devraient être établies pour assurer que les contenus de la bibliothèque médiatique contenant les données sont répertoriés systématiquement, que tout écart divulgué par un répertoire physique est remédié au moment opportun et que des mesures sont prises pour maintenir l'intégrité des médias magnétiques enregistrés dans la bibliothèque.

14. Les procédures de secours pour les médias devraient inclure l'enregistrement approprié des fichiers de données et des logiciels. Les sauvegardes devraient être enregistrées de façon sécuritaire et les sites de stockage devraient être périodiquement examinés au chapitre de la sécurité d'accès physique et de la sécurité des fichiers de données et des autres articles.

SÉCURITÉ PHYSIQUE

15. Des mesures appropriées de sécurité physique et de contrôle d'accès devraient être établies conformément à la politique de sécurité générale. L'accès devrait être restreint aux individus qui ont été autorisés à avoir un tel accès.

16. Des mesures suffisantes devraient être mises en place et maintenues pour une protection contre les facteurs environnementaux (p. ex., incendie, poussière, électricité, chaleur et humidité excessive). Un matériel et des appareils spécialisés devraient être installés pour surveiller et contrôler l'environnement.

17. Des batteries et/ou des génératrices UPS devraient être installées pour se protéger contre les pannes ou les fluctuations d'électricité.

ANNEXE C

LISTE DE PERSONNES INTERROGÉES

- Louise Bédard, administratrice de bases de données
- Gilles Lacroix, gestionnaire technique
- Patti Pomeroy, gestionnaire, Services informatiques de la Direction des corporations
- Martino Rafael, administrateur de LAN
- Jean-Pierre Lafrance (conseiller), soutien informatique