CHRONIQUE DE SÉCURITÉ

NUMÉRO SPÉCIAL « MAUVAISES PRATIQUES ET SOLUTIONS ASSOCIÉES »
1RE PARTIE

Décembre 2004, Volume 1 - Numéro 5

Que d'effervescence dans le réseau au cours des deux derniers mois ! Des plans d'actions, nous sommes passés à l'action en matière de sécurité. Des groupes de travail ont été constitués dans chacun des réseaux locaux, déterminés à documenter des mesures de sécurité. Merci pour votre implication et bonne lecture !

Laurent Fey.

MESURES DE SÉCURITÉ

Des activités régionales ont été organisées par l'Agence de santé et services sociaux Chaudière-Appalaches, en septembre et en octobre. Ces activités de soutien et d'accompagnement pour l'élaboration et la mise en place de mesures issues de consensus de priorisation par réseau local ou regroupement d'autres types d'établissements se poursuivront au cours de l'hiver. Ces travaux visaient à nous approcher de la conformité demandée par le ministère de la Santé et des Services sociaux pour le 31 décembre 2004. Cette date a été repoussée au 31 mars 2005 et des ajustements au document final ont été apportés au cours de la rencontre provinciale de novembre dernier. Ce document du Ministère vous sera transmis dès sa réception à l'Agence. La théorie des « petits pas » chère à M. Pierre Desbiens, notre coordonnateur régional, devrait à nouveau se révéler exacte.

Voici donc les mesures pour lesquelles les travaux de documentation par CSSS devraient se poursuivre :

- Gestion des mots de passe
- Politique de sécurité
- Accès aux locaux informatiques et salles de télécommunications
- Copies de sauvegarde
- Gestion des anti-virus

Des activités régionales vont se mettre en place au cours du mois de décembre relativement à la catégorisation, à l'évaluation commune des risques et des menaces, et aux procédures d'escalades.

Je tiens particulièrement à souligner l'engagement du CSSS de la région de Thetford et je les remercie de leur participation à des travaux régionaux liés à la catégorisation des actifs. Oui, notre dynamique existe et elle est bien présente.

Enfin, il reste toujours un brin d'optimisme concernant un éventuel financement du dossier sécurité de la part du Ministère, la période des fêtes de fin d'année étant propice aux cadeaux !

Sommaire :

Agence de développement de réseaux locaux de services de santé et de services sociaux
Québec
Chaudière–Appalaches

PRÉVENTION CONTRE LE VOL

Six anciens établissements de la région et l'Agence ont choisi de poser les premiers gestes en matière de prévention contre le vol en participant à une commande régionale de marquage anti-vol et de câbles de fixation d'équipements auprès de la compagnie StopOxygen.
Au total, près de cent trente équipements portables vont être identifiés par une plaque de type « compugard » comme appartenant au réseau de la santé et des services sociaux de la région de la Chaudière-Appalaches. Chaque équipement identifié sera référencé dans une base de données internationale accessible dans Internet. La gestion de cette base et son coût de fonctionnement sont assumés par l'Agence pour l'année 2005.

COLLOQUE SÉCURIS@NTE 5.0

Colloque SécuriS@nté 5.0
« En sécurité informatique ... mieux vaut savoir jouer que d'être déjoué ! »

Pour sa cinquième édition, le Colloque SécuriS@nté 5.0 se déroulera le 6 mai 2005 à l'Hôtel Plaza Québec. Le thème principal cette année est *Mieux vaut savoir jouer que d'être déjoué !* Le « Hacking » sera au cœur des débats. Si vous avez visité le site SécuriS@nté 5.0 (www.chuq.qc.ca/securisante), vous avez pu lire qu'un des invités n'est autre que le célèbre Kévin Mitnick, surnommé le « Condor ». Cet homme est peut-être le plus grand hacker de notre ère : piratage téléphonique, ingénierie sociale de grande envergure, infiltration au Federal bureau of investigation, etc. Kevin Mitnick, âgé de 40 ans, a passé 5 ans en prison. À l'époque de son procès, il a été accusé d'avoir causé au total dix millions de dollars de dégâts en s'en prenant à plusieurs réseaux d'entreprise. Il est aujourd'hui sorti de prison. Il est un consultant en sécurité de grande renommée et auteur d'un premier ouvrage, « *L'art de la supercherie* », qui traite principalement de l'ingénierie sociale. Le colloque sera donc une bonne occasion de le rencontrer !

CARTOGRAPHIE DES SYSTÈMES D'EXPLOITATION

Un courriel personnalisé a été envoyé à chaque établissement, il présente la cartographie globale de la région et de chaque centre de santé et de services sociaux (CSSS).

Voici quelques chiffres pour votre information :

Environ 3700 postes sont répartis dans la région : 50 postes en Windows 95, 50 en Windows 98, 100 en Windows Nt4, 2300 en Windows 2000, 1100 en Windows Xp. À noter que Linux a fait son entrée dans la région : 36 postes à ce jour.

Comme vous pouvez le constater, le parc informatique régional est constitué à 90 % d'un environnement Windows 2000/XP. Ce qui nous permet d'ores et déjà de constater que les configurations matérielles sont plus que performantes.

« MAUVAISES PRATIQUES ET SOLUTIONS ASSOCIÉES », 1RE PARTIE

La majorité des incidents de sécurité que nous vivons au quotidien sont souvent issus d'un petit nombre de mauvaises pratiques bien connues dans le domaine de la sécurité. Des nos jours, de nombreux éléments nous permettent de dire que les différentes attaques que nous pouvons subir ne sont pas attribuées à la compétence des pirates et à leur intelligence, mais bien à notre manque de temps et d'argent, à nos impératifs opérationnels, à nos vulnérabilités et, parfois même, à nos négligences.
En 2002, les experts en sécurité estimaient à 64 % les incidents de sécurité imputables à des erreurs de manipulation. Nous allons en parcourir quelques-unes et vous livrer des astuces pour les éviter.

Face aux nouvelles menaces virales

On sait bien qu'il ne suffit pas d'avoir un anti-virus pour être protégé ! Aujourd'hui, le « talon d'Achille », c'est le réseau. En effet, un anti-virus peut contrôler des fichiers, des disques durs, mais pas des accès au réseau. L'infection est détectée lorsque le ver a déjà infecté le système. Face à ce type de menaces, une des premières bonnes pratiques à mettre en place consiste à être très rigoureux sur l'application des correctifs de sécurité et, lorsque cela est possible, à protéger ces mêmes systèmes par la mise en place de coupe-feu.

Un coupable bien identifié : le mot de passe

La gestion des mots de passe, ou plutôt leur non-gestion, est la première cause d'incidents de sécurité. Mal choisis ou même laissés par défaut, les mots de passe sont le point faible d'un grand nombre d'organisations. Des statistiques de consultants en sécurité révèlent que 90 % des systèmes disposent d'accès avec des mots de passe définis par défaut. Pour être plus précis, ces mêmes études affirment que les mots de passe des applications les plus utilisées (Oracle, Sql serveur, etc.) sont rarement changés une fois les installations terminées. Et lorsqu'ils le sont, ce sont pour des valeurs très simples à deviner, telle une variation du nom de l'entreprise ou les incontournables *« test »* , *« admin »* ou *« essai »*. Je lis un sourire sur votre visage ! Bilan : plusieurs milliers de machines ont été infectées dans le monde au cours des derniers mois et autant de bases de données dérobées. Je n'aborderai pas le quotidien des utilisateurs; la réalité, vous la connaissez aussi bien que moi !

Les solutions :

- S'assurer que les mots de passe sont réellement personnalisés ou désactivés (dans le cas de comptes inutilisés).
- Sensibiliser les utilisateurs en s'assurant d'avoir une politique suffisamment efficace pour ne pas les encourager à la contourner : un mot de passe composé de chiffres, de lettres et changé une fois par trimestre représente une façon de faire raisonnable.
- Une solution de SSO (Single Sign-On) ou « authentification unique » évite la multiplication des mots de passe pour chaque utilisateur : il suffit de s'authentifier auprès du client SSO pour avoir accès à l'ensemble des applications de l'organisation. Cette dernière solution est la plus onéreuse.

L'administration des sauvegardes

Des bonnes sauvegardes représentent l'assurance de pouvoir reprendre l'activité au plus vite après un accident majeur. Pour plusieurs, les sauvegardes sont la seule parade efficace contre les incidents de sécurité. Mais la réalité sur le terrain est toute autre ! Le plus difficile n'est pas de mettre en place un système de sauvegarde, mais surtout de le faire évoluer. Les volumes et les espaces disque sont amenés à grossir et, parfois, on se retrouve avec des systèmes de sauvegarde incapables de jouer leur rôle à cause de cette augmentation de volume. La prise en charge et la sortie des bandes sont des aspects à ne pas négliger, surtout sur les sites distants lorsque les opérations de sauvegarde sont faites par du personnel de bureau à qui on demande de changer quotidiennement les cartouches. Mais, que faire alors ?

Se diriger vers une approche automatisée est une bonne solution. Mais, il est impératif de désigner un responsable des opérations de sauvegarde qui devra contrôler le fonctionnement de la solution installée, s'assurer du bon état des sauvegardes en procédant à des tests de récupération et, surtout, gérer le flux des supports en faisant en sorte qu'ils soient régulièrement changés et sortis des locaux.

Nos chers collègues de travail qui ne partent jamais !

Ici, nous faisons face à un problème purement organisationnel. Le manque de communication entre le service informatique et le service des ressources humaines est vraiment à regarder de près. Il est courant de constater qu'on se retrouve avec des accès réseau attribués à des stagiaires ou des prestataires externes, ou encore à nos propres collègues qui ont quitté l'organisation depuis plus de six mois. Ces accès sont inutiles et potentiellement dangereux : le collaborateur ou un pirate peuvent revenir à loisir et détourner les accès sans attirer l'attention.

La solution :

Il est fondamental d'unifier les procédures d'arrivée et de départ du personnel, en incluant systématiquement le service informatique dans le processus : il doit être avisé de tous les départs; de cette façon, il pourra procéder à la fermeture des comptes et au retrait des privilèges des personnes n'appartenant plus à l'organisation.

Le paramétrage des logiciels

La simplicité actuelle d'installation de nos programmes informatiques nous fait parfois oublier l'importance du paramétrage. Les réglages par défaut laissent souvent des portes grandes ouvertes. La règle de base étant de ne pas mettre un outil en production tant que l'on en a pas vérifié les paramètres. Mais, les vérifier n'est pas suffisant, il est indispensable d'évaluer clairement ses besoins au préalable. Il convient donc à chacun de se poser un minimum de questions : Le paramétrage est-il universel ? Est-il cohérent avec la topologie de mon réseau ? Quels sont mes besoins de contrôle d'accès ?

À suivre dans le prochain numéro...

Source : Direction des ressources financières, matérielles et informationnelles
Courriel : Laurent.Fey@ssss.gouv.qc.ca
ISSN : 1710-5692
Dépôt légal — Bibliothèque nationale du Canada, 2004
Bibliothèque nationale du Québec