Note from ICDPPC Secretariat
This is a translation of a proposed resolution. There may have been changes to the resolution when it was adopted.

26ème Conférence Internationale de Protection de la Vie Privée
et des Données Personnelles
Wroclaw, 14 – 16 septembre 2004

Proposition de modification de la Résolution de la Conférence 2003 concernant les mises à jour automatiques des logiciels

Résolution

Le Bureau du Commissaire fédéral australien de protection de la vie privée, le Commissaire à l'information et la vie privée de l'Ontario (Canada), le Commissaire à la protection de la vie privée de Hongkong et le Commissaire à la protection des données et de l'accès à l'information du Land de Brandebourg proposent que la Conférence adopte la présente résolution:

1. La conférence constate avec inquiétude que les fabricants de logiciels du monde entier utilisent de plus en plus des techniques non transparentes pour la mise à jour des logiciels présents dans les ordinateurs de leurs utilisateurs. Cette pratique leur permet de:
   - lire et de recueillir des informations personnelles mises en mémoire sur l'ordinateur de l'utilisateur (par ex. des réglages de navigateur Web et des indications sur le furetage habituel de l'utilisateur) sans que celui-ci soit en mesure de remarquer, d'influencer ou d'empêcher ce type d'interférence,
   - exercer un contrôle, au moins partiel, sur l'ordinateur visé et, ce faisant, limiter la capacité qu'a l'utilisateur de se conformer à ses obligations et d'exercer ses responsabilités, en tant que personne censé contrôler la sécurité des données personnelles, quelles qu'elles soient, qu'il peut avoir à traiter,
   - changer le logiciel installé sur l'ordinateur qui sera ensuite utilisé, sans qu'aucun test ne soit effectué ou aucune autorisation ne soit requise,
   - provoquer, en faisant la mise à jour du logiciel, des défaillances techniques dans l'ordinateur, sans qu'il soit possible de déceler que celle-ci en est la cause.

Ceci peut provoquer des problèmes particuliers pour les institutions gouvernementales et pour les entreprises privées qui ont des obligations légales spécifiques relatives au traitement des données personnelles.

2. La Conférence demande aux entreprises fabricant des logiciels (software companies) de:
   a. offrir des procédés permettant de mettre à jour le logiciel en ligne qui ne puissent pas être opérationnels sans en aviser l'utilisateur et sans avoir obtenu son consentement, sans excéder l'étendue de ce consentement, de façon transparente et sans permettre l'accès à l'ordinateur à l'insu de l'utilisateur;
   b. Ne demander la communication de données personnelles que si l'utilisateur l'autorise en toute connaissance de cause et seulement dans la mesure où cela est nécessaire pour la mise à jour en ligne. Les utilisateurs ne devraient pas être obligés de s'identifier (ce qui diffère de la nécessité d'authentifier leur droit d'accès à ce service) avant de pouvoir engager le processus de téléchargement,
   c. Offrir un service de mise à jour en ligne qui permette d'effectuer un test sur un serveur détaché avant d'être installé.

3. La Conférence encourage le développement et la mise en oeuvre de techniques d'actualisation des logiciels qui respecte la vie privée et l'autonomie des utilisateurs.

Notes explicatives

L'objectif du présent document est de fournir quelques informations de base sur les amendements proposés pour la résolution adoptée par les Commissaires pendant la Conférence de 2003 concernant la mise à jour automatique des logiciels. La résolution était proposée par Alexander Dix et fondée sur les travaux du Groupe de travail International pour la protection des données dans les télécommunications. La résolution est appelée "Résolution N°4" et se trouve sur le site des résolutions de la Conférence 2003:
www.privacyconference2003.org/commissioners.asp

La résolution 2003 avait exprimé une inquiétude en ce qui concerne la non transparence des techniques de mise à jour des logiciels présents dans les ordinateurs des utilisateurs, et qui donnent aux fabricants des logiciels la possibilité de contrôler et d'accéder en partie aux informations conservées dans les ordinateurs des utilisateurs.

Depuis la publication de la résolution, Microsoft a été en contact avec plusieurs commissaires, parmi eux Alexander Dix, Ann Cavoukian, son adjoint Ken Anderson et l'ancien commissaire fédéral australien de la protection de la vie privée Malcolm Crompton. Microsoft avait expliqué de façon convaincante qu'une partie de la résolution, telle qu'elle a été adoptée par la Conférence 2003, était non seulement impossible à mettre en œuvre, mais aussi contre-productive. Par contre-productive on entend que la mise en oeuvre de la résolution pourrait retarder certaines mises à jour même lorsqu'elles sont nécessaires et urgentes.

La nécessité d'une mise à jour rapide repose sur le fait que la plupart des virus et des attaques de pirates ont lieu après la mise à jour. Les pirates et les créateurs de virus trouvent souvent les faiblesses des logiciels grâce à la structure de mise à jour de ces mêmes logiciels, en identifiant ce en quoi consiste les réparations. Dans ces circonstances il est extrêmement important de fournir une mise à jour du logiciel (appelée parfois le patch) à un maximum d'utilisateurs et le plus rapidement possible. Cela évite que les pirates et les créateurs de virus ne bénéficient d'un laps de temps entre la mise à disposition du public de la mise à jour et son adoption par tous,

période qu'ils pourraient utilisée pour inventer des virus capables d'attaquer les points faibles des logiciels. Littéralement chaque heure de retard augmente le risque de provoquer des dégâts dans le monde entier.

Interdire la mise à jour rapide des logiciels peut fragiliser la protection de la vie privée en donnant aux pirates une opportunité d'accéder aux données personnelles dans les ordinateurs des personnes physiques.

A ce propos Microsoft a rédigé un certain nombre de remarques concernant la résolution 2003 dans lesquelles il explique comment la résolution peut être contre-productive.

Microsoft constate que:

> "Puisque la distribution rapide des patchs est essentielle pour protéger la santé de l'Internet et la vie privée des utilisateurs, on ne peut choisir le cédérom comme moyen de diffusion (par conséquent la partie de la résolution qui n'encourage pas les actualisations en ligne est très problématique). Tout d'abord, la distribution par cédérom ne peut pas être effectuée suffisamment rapidement, en particulier si les virus sont expédiés dans un laps de quelques heures après la publication du bulletin. Deuxièmement, le cédérom est gravé à un moment précis, et peut ne plus être actuel au moment de son installation par l'utilisateur (exemple : le patch peut être déjà modifié ou de nouveaux patchs peuvent être déjà publiés). Malgré que l'expédition de cédérom possède une valeur certaine (spécialement pour les très grands patchs ou pour fournir une mise à jour à un système non conforme, sous forme de plusieurs packs et/ou patchs de service), seules les mises à jour en ligne peuvent assurer aux utilisateurs la possibilité d'installer les patchs les plus récents avant qu'un virus ne paralyse leur logiciel ou qu' un pirate n'accède à leur ordinateur sans autorisation pour voler le "PII" (Programme Integrated Information).
>
> Nous ne comprenons pas bien non plus pourquoi les patchs doivent être fournis uniquement à la demande ou à l'initiative de l'utilisateur au lieu de fournir l'information et le choix selon les préférences ("notice and choice") à l'utilisateur final. Nous savons, bien sûr, que certains automobilistes ne bouclent pas leur ceinture de sécurité bien qu'il sache que conduire sans ceinture peut entraîner la mort ou des dégâts physiques sérieux (sans parler, dans certaines pays, des sanctions imposées par la police!). A la lumière de cette réalité, la procédure qui requiert l'information et le choix permettrait de conserver un équilibre entre la protection de la vie privée à l'aide des patchs et le contrôle de l'utilisateur.
>
> Finalement, nous proposons de remplacer le texte concernant l'accès à l'ordinateur à l'insu de l'utilisateur ("unchecked access"), principalement parce qu'il n'est pas clair. Le système opérationnel (OS) lui-même a un accès au système à l'insu de l'utilisateur, il n'y pas beaucoup de sens de suggérer une mise à jour (surtout au noyau du OS) qui ne soit pas capable de contrôler l'accès. De plus, si le point faible à réparer permet un accès (du niveau de l'administrateur du système), alors le vendeur du logiciel, le criminel, ou quelqu'un avec la

connaissance et le savoir technique suffisant peut avoir un accès au système à l'insu de l'utilisateur ("unchecked access"); c'est pourquoi les patchs sont tellement importants."[1].

En réponse aux commentaires de Microsoft, Alexander Dix a travaillé avec Microsoft sur une proposition de modification de la résolution. L'objectif était de préserver la protection de la vie privée de la résolution initiale, tout en la rendant plus fonctionnelle. Finalement, Alexander Dix a proposé un projet de modification de la résolution.

La résolution modifiée a été envoyée par courrier électronique aux Commissaires le 12 avril 2004, accompagnée d'une lettre du Commissaire fédéral australien Malcolm Crompton expliquant les raisons d'une telle proposition. Cependant seules 8 réponses ont été reçues. On a alors décidé de soumettre de nouveau la résolution à la conférence pour assurer un consensus plus fort.

La proposition de modification de la résolution de la Conférence 2003 est la suivante. Au lieu de:

"la conférence demande aux fabricants de logiciels de respecter les conditions suivantes :

- offrir des procédés permettant de mettre à jour le logiciel en ligne, seulement lorsque l'utilisateur en prend l'initiative ou la requiert, d'une façon transparente et sans que soit avalisé, par la même occasion, l'accès aux informations contenues dans l'ordinateur de l'utilisateur ,
- ne demander la communication de données personnelles que si l'utilisateur l'autorise en toute connaissance de cause et seulement dans la mesure où cela est nécessaire pour la mise à jour en ligne. Les utilisateurs ne devraient pas être obligés de s'identifier (qui diffère de la nécessité d'authentifier leur droit d'accès à ce service) avant de pouvoir engager le processus de téléchargement,
- n'offrir la possibilité de choisir la mise à jour en ligne que comme une alternative à d'autres moyens fournis « hors-ligne » pour les obtenir, tels que les cédéroms."

Le texte modifié:

"La Conférence demande aux entreprises fabricant des logiciels de respecter les conditions suivantes :

a. offrir des procédés permettant de mettre à jour le logiciel en ligne qui ne puissent pas être opérationnels sans en aviser l'utilisateur et sans avoir obtenu son consentement, sans excéder

[1] Extraits de la lettre envoyée par Scott Charney de Microsoft à Ann Cavoukian. Le 12 avril 2004 la lettre a été envoyée par courrier électronique par le Commissaire fédéral australien Malcolm Crompton aux commissaires qui participèrent à l'élaboration des résolutions de la Conférence 2003 des commissaires à la protection de la vie privée.

l'étendue de ce consentement, de façon transparente et sans permettre l'accès à l'ordinateur à l'insu de l'utilisateur;

b. (aucune modification)

c. Offrir un service de mise à jour en ligne qui permette d'effectuer un test sur un serveur détaché avant d'être installé. "

En tant qu'organisateur de la Conférence 2003, le Commissaire fédéral de protection de la vie privée d'Australie propose cette résolution avec le soutien des commissaires de Brandebourg, Ontario et Hongkong. Les commissaires d'Irlande, d'Espagne, le commissaire fédéral d'Allemagne, du Pays Bas et le contrôleur européen de la protection des données apportent également leur soutien aux modifications distribuées en avril 2004.

Si la Conférence approuve les modifications de la résolution, nous bénéficieront d'un fort soutien de la part de l'industrie dans la mise en oeuvre de la résolution modifiée, Microsoft en tête. Ceci constituerait un exemple exceptionnel d'application pratique de la protection de la vie privée, puisque le travail des commissaires aurait alors une incidence profonde sur le monde des affaires.