CNRS/FSD/Sécurité des Systèmes d'Information

Recommandations pour l'utilisation des services gratuits sur Internet

En date du 17 avril 2008
Référence 08.1841/FSD

Nature du document : Recommandations

Destinataires :

- directeurs d'unité
- responsables informatiques
- tous utilisateurs

Mise en œuvre : Ces recommandations sont d'application générale. Il est toutefois souhaitable qu'elles soient explicitement intégrées dans la politique de sécurité des systèmes d'information de l'unité. Cette politique pourra préciser le cas échéant, en fonction des particularités de l'unité, les dérogations possibles à ces recommandations et en contre partie les moyens permettant de viser un niveau acceptable et contrôlé de sécurité.

Version 1.0

Recommandations

L'utilisation à des fins professionnelles des nombreux services gratuits disponibles sur Internet (messagerie électronique, hébergement de sites web, stockage de données,…) suscite de manière générale de sérieuses réserves.
En toute rigueur, l'externalisation d'un service n'est concevable que dans le cadre d'un contrat où juridiquement toutes les implications auront bien été étudiées et où techniquement toutes les mesures destinées à assurer la disponibilité, l'intégrité et la confidentialité des informations auront été correctement mises en œuvre. Il est bien évident que l'on ne peut attendre de telles garanties d'un fournisseur de service gratuit. Les risques sont accrus lorsque ce fournisseur est situé à l'étranger.

Messagerie électronique

Sauf circonstances particulières requérant un certain anonymat l'utilisation à des fins professionnelles d'un service de messagerie gratuit (Gmail par exemple) est à proscrire.
L'adresse de messagerie, utilisée à titre professionnel (adresse utilisée pour définir l'expéditeur d'un message ou communiquée aux contacts professionnels) doit être celle fournie par l'organisme d'appartenance.
Pour des raisons de visibilité et de réputation, l'adresse électronique professionnelle ne doit jamais être celle d'un fournisseur gratuit.
L'adresse électronique définie dans les différentes bases de données ou annuaires du CNRS pour référencer une personne travaillant au CNRS ne doit donc jamais être celle d'un fournisseur gratuit. Il en est de même pour l'adresse électronique définie dans un certificat électronique délivré par le CNRS.
Aux responsables des systèmes d'information, il est rappelé que la meilleure façon d'éviter que les utilisateurs ne soient tentés de recourir à des services externes est de fournir en interne un service de qualité. Concrètement cela signifie que les boites aux lettres doivent être de taille suffisante (typiquement quelques Go par utilisateur). De même il convient de déployer les outils et protocoles permettant de gérer à distance et de façon sécurisée la messagerie :

- webmail sécurisé en HTTPS (Horde/IMP, SquirrelMail, etc.) ;
- protocoles sécurisés IMAPS et POP3S pour la consultation de messages ;
- SMTPS pour l'envoi de messages.

Il peut arriver que dans des situations particulières, un agent soit conduit à utiliser, hors de son bureau, une adresse personnelle et un fournisseur externe pour un motif professionnel (en cas d'indisponibilité du serveur mail par exemple, ou pour des raisons de discrétion ou d'anonymat). En aucun cas les données transitant de cette façon ne devront comporter en clair (sans chiffrement robuste) des données sensibles.

Hébergement de site web

Ne serait-ce que pour des raisons de sécurité, en aucun cas un site web institutionnel ne doit être hébergé chez un fournisseur gratuit.
Pour des raisons de visibilité et de réputation, l'adresse utilisée pour accéder à un site web doit être une adresse institutionnelle et non celle de l'hébergeur éventuel.

Externalisation du stockage

Il y a lieu de rappeler un principe de sécurité fondamental : une donnée interne à l'organisme ne doit jamais transiter ou être stockée à l'extérieur à moins qu'elle ne soit convenablement chiffrée ; qui plus est lorsque l'on utilise des services gratuits.
Ainsi utiliser des services gratuits externes comme outils de travail collaboratif est à éviter absolument. Il faut choisir d'autres méthodes qui n'exposent pas de façon incontrôlée des informations sensibles à l'extérieur.
De même il est proscrit d'accéder à des informations un tant soit peu sensibles depuis une machine en libre service dans un cybercafé, un hôtel ou autre lieu public
Face à la demande pressante et souvent légitime des utilisateurs qui souhaitent accéder à leurs données depuis n'importe quelle machine et tout point du monde, des solutions doivent être proposées par l'organisme.
Il est parfaitement acceptable de transporter des données correctement chiffrées sur son ordinateur portable. Il en est de même pour accéder aux données situées sur un serveur de son laboratoire, depuis son ordinateur portable en utilisant un protocole sécurisé, c'est-à-dire avec authentification et chiffrement. La mise en place d'un réseau privé virtuel (VPN) est parfaitement adaptée à cette situation.

Web 2.0

Chacun a sa propre définition du terme de Web 2.0 mais beaucoup s'accordent sur l'une des caractéristiques qui est de regrouper de nouveaux usages d'Internet où chaque individu est aussi producteur d'informations.
La plus grande prudence est requise lorsque l'on est amené à fournir des informations personnelles sur Internet. Si la divulgation d'informations à caractère privé relève du libre arbitre de chacun, il faut bien mesurer toutes les conséquences pour l'organisme et non seulement l'individu de la fuite d'informations de nature professionnelle. La fréquentation des sites communautaires (blogs, wiki, etc.), des réseaux sociaux (comme FaceBook) doit donc se faire avec la plus grande responsabilité.
Avant tout, il faut faire preuve d'esprit critique et de bon sens en se posant les bonnes questions. Est-ce compatible avec la politique de l'organisme ? N'y a-t-il pas des risques concernant la sécurité de l'information ? Une fois diffusée sur Internet une information ne peut plus être rétractée.

Aujourd'hui différents fournisseurs offrent sur Internet de nombreux services gratuits. Avec l'avènement de ce que certains on appelé le « web 2.0 », la palette des services et des usages s'est encore élargie : le courrier électronique, la messagerie instantanée, les moteurs de recherche, la téléphonie, la téléconférence, l'hébergement de sites web, les blogs, la gestion d'agenda, le stockage et le partage de documents, les sites communautaires ou bien encore les réseaux sociaux. Parmi les plus connus on peut citer : Google[1], Gmail[2], Hotmail[3], Yahoo[4], Free[5] , MySpace[6], LinkedIn[7] , Facebook[8], You Tube[9], Skype[10], Doodle[11].
Ces services sont généralement bien conçus, de bonne qualité, avec une excellente ergonomie. Les espaces de stockage fournis sont souvent conséquents (plusieurs Go). Avec leur interface web ils sont accessibles de partout, depuis n'importe quelle machine. Si séduisants soient-ils, peut-on les adopter sans discernement dans un contexte professionnel ?

Usage professionnel

L'usage de ces services gratuits dans un cadre professionnel soulève de nombreuses questions. Certes ils permettent d'accéder à des services réellement utiles qui peuvent ne pas être fournis localement par le service informatique. Mais il s'agit simplement parfois de contourner les restrictions imposées par la politique de sécurité des systèmes d'information.
Pour utiliser ces services, il faut s'inscrire, fournir un certain nombre d'informations et approuver sans pouvoir les négocier les clauses du contrat. La pratique veut que l'on clique généralement sur le bouton « J'accepte », sans lire les conditions ni même savoir si l'on est réellement habilité à s'engager. Il est cependant très instructif de parcourir les termes du contrat qui accompagne la fourniture du service. Ainsi les conditions d'utilisation de Gmail[12] précisent : *« Le Service est mis à votre disposition pour un usage exclusivement personnel. »* ce qui implicitement exclut un usage professionnel.

Quelle gratuité ?

Ces fournisseurs de services agissent rarement par philanthropie. Dans un monde où règne le virtuel, derrière une apparente gratuité, il y a de l'argent bien réel à gagner. Pour s'en convaincre il suffit d'observer la capitalisation boursière de certains acteurs. Parfois il ne s'agit que de simples produits d'appel pour des services payants, ce qui en limite l'intérêt et risque d'entrainer par la suite une coûteuse dépendance. Mais généralement le modèle économique de ces services gratuits repose sur la vente de publicités ciblées en fonction du profil des utilisateurs. Par exemple il est précisé dans les règles de confidentialité de Gmail[13] : *« Le service Gmail comprend des publicités et des liens contextuels basés sur l'adresse IP, le*

[1] http://www.google.fr/
[2] http://www.gmail.com
[3] http://www.windowslive.fr/hotmail/
[4] http://fr.yahoo.com/
[5] http://www.free.fr
[6] http://www.myspace.com/
[7] http://www.linkedin.com
[8] http://www.facebook.com/
[9] http://fr.youtube.com/
[10] http://www.skype.com/intl/fr/
[11] http://www.doodle.ch/
[12] http://mail.google.com/mail/help/intl/fr/terms_of_use.html
[13] http://mail.google.com/mail/help/intl/fr/privacy.html

contenu des messages et d'autres informations liées à votre utilisation de Gmail. » Outre le fait que cette publicité puisse en détournant l'attention entrainer une perte de productivité, l'idée qu'un profil de l'utilisateur soit établi et conservé fait frémir. Facebook[14] va encore plus loin puisque ses pratiques reviennent à introduire le commerçant dans le cercle d'amis. La CNIL s'inquiète de telles pratiques et appelle à la vigilance[15].
D'autres modèles se rapprochent du parasitisme. Ainsi Skype utilise les ressources en bande passante et en puissance de calcul fournies par les utilisateurs pour se bâtir un réseau privé virtuel mondial sans financer aucune infrastructure. En effet le fait d'installer sur une machine le produit de Skype qui permet de téléphoner « gratuitement » transforme cette machine en un nœud du réseau Skype sans que son propriétaire puisse contrôler réellement le trafic échangé.
Par ailleurs il faut se demander quelles garanties offre un service gratuit. Même si l'on peut penser que le fournisseur fera de son mieux, il n'y a aucun engagement de sa part. Ainsi dans les conditions d'utilisation de Gmail il est précisé : « *En outre, vous comprenez et acceptez que le service est proposé EN L'ÉTAT et SOUS RESERVE DE DISPONIBILITÉ. Google décline toute responsabilité quant à la disponibilité, la rapidité, la sécurité ou la fiabilité du Service. Google se réserve aussi le droit de modifier, de suspendre ou d'interrompre le Service avec ou sans préavis, à tout moment et sans aucune responsabilité à votre égard.* »
Est-il bien raisonnable de faire reposer un service aussi vital que la messagerie électronique sur un fournisseur probablement de bonne volonté mais qui n'offre aucune garantie contractuelle ? Que se passera-t-il pour celui qui a confié tous ses messages, toutes ses données à un fournisseur gratuit qui arrête son service ou disparait ? Il faut espérer qu'il a à sa disposition une sauvegarde fiable.
Cela est si vrai que Google offre, à l'usage des entreprises, un service payant avec une garantie de disponibilité à 99.9% pour la messagerie[16]. C'est une preuve supplémentaire que le service gratuit est insuffisant pour celles-ci.
Il est donc important de bien réfléchir aux coûts cachés derrières ces services gratuits. Il ne faut pas non plus surestimer certains avantages. Lorsqu'un disque de 500Go coûte de l'ordre de 100€, il faut relativiser le fait de pouvoir stocker quelques Go sur un serveur gratuit.

Confidentialité

Le respect de la confidentialité des messages transmis, des informations stockées n'est absolument pas garanti. Il faudrait être bien naïf pour croire que lorsque le service est hébergé dans un état étranger, des informations ne seront jamais communiquées aux services de renseignement de celui-ci. D'ailleurs Google écrit toujours dans ses conditions d'utilisation[17] :
« Google se réserve également le droit d'accéder, de lire, de conserver, et de communiquer toute information dont elle pense raisonnablement qu'elle est nécessaire aux fins de (a) respecter toute obligation légale ou réglementaire applicable, ainsi que toute demande d'une autorité judiciaire ou toute autre autorité publique; […] »
Par ailleurs, il faudrait vérifier qu'en externalisant ainsi ses informations, on respecte bien les différentes réglementations concernant les flux transfrontières de données.
Hushmail[18] offre bien un service gratuit de courrier électronique chiffré. Cependant comme le montre un article de Wired[19], la confidentialité est loin d'être absolue puisque la société admet pouvoir fournir sur requête judiciaire le moyen de déchiffrer les messages.

[14] http://www.facebook.com/business/
[15] http://www.cnil.fr/index.php?id=2383
[16] http://www.google.com/a/help/intl/fr/admins/sla.html
[17] http://mail.google.com/mail/help/intl/fr/terms_of_use.html
[18] http://www.hushmail.com/
[19] http://blog.wired.com/27bstroke6/2007/11/hushmail-to-war.html

L'idée qui consiste à dire, utilisons ces services gratuits mais chiffrons les données pour en assurer la confidentialité soulève plusieurs objections. Si nous prenons l'exemple de la messagerie électronique, le chiffrement étant de la responsabilité de l'expéditeur du message, demandant une action volontaire de sa part et nécessitant d'avoir récupéré au préalable la clé publique du destinataire, il est bien évident que cette solution n'est pas réaliste. Comme seul le corps des messages est chiffré, les en-têtes qui contiennent notamment l'expéditeur, les destinataires et l'objet du message sont une source d'information extrêmement précieuse lorsque l'on recoupe les différents messages échangés pour déterminer les centres d'intérêt et les relations d'une personne. De plus il n'est pas possible de lire des messages chiffrés en se connectant à l'aide d'un navigateur sur l'interface web du service de messagerie, ce qui en retire l'un des atouts qui est de pouvoir accéder à sa messagerie depuis n'importe quelle machine. Enfin il douteux que les fournisseurs de services acceptent longtemps un comportement qui va l'encontre de leur propre intérêt qui est de vendre de la publicité en fonction du contenu des messages.
Certes la confidentialité d'un message non chiffré est toute relative car il est toujours susceptible d'être intercepté lorsqu'il est transféré sur le réseau. Cependant il est nettement plus facile et efficace de récupérer sur un serveur l'ensemble des messages échangés pendant une longue période que d'installer des interceptions aux différents endroits où peuvent transiter les messages. De plus l'interception d'un courrier interne qui reste sur le réseau interne est nettement plus difficile que s'il transite par un serveur externe.
Le problème de confidentialité ne concerne pas uniquement les services gratuits. Par exemple le célèbre BlackBerry de Research in Motion est l'objet de réels doutes.
Pour de multiples raisons, les outils de travail collaboratifs n'ont pas pris, du moins dans notre milieu, l'essor attendu. Cela est probablement dû à leur trop grande complexité, tant dans la mise en œuvre que dans l'utilisation ainsi qu'au coût élevé des produits disponibles. La fourniture dans le domaine par Google, entre autres, de services gratuits disponibles à partir d'un simple navigateur risque de changer la donne. Ainsi Google Document[20] permet de stocker et partager ses documents sur un serveur externe. L'accessibilité des documents depuis n'importe quelle machine connectée à Internet et la possibilité de les partager est extrêmement séduisante. Cependant le simple bon sens exige de se poser les questions habituelles, quelle garantie de disponibilité, d'intégrité et de confidentialité est assurée. La réponse est évidemment aucune et il ne faut donc pas l'utiliser. Même un agenda partagé comme Google Agenda[21] ou une simple gestion de réunion comme Doodle[22] contiennent des informations trop sensibles pour que l'on puisse se permettre de risquer une divulgation.
Pour s'envoyer des documents au sein de l'organisme et pour pallier les limitations dans la taille des fichiers attachés transmis par courrier électronique, il peut être tentant d'utiliser un service gratuit d'envoi de fichier comme celui de Free[23]. Si pour les photos de vacances cela ne porte pas vraiment à conséquence, il n'en est évidemment pas de même s'il s'agit d'échanger un document confidentiel. Il serait certainement possible de fournir un service analogue en interne mais une solution reposant sur un partage de fichiers sur le réseau est probablement meilleure et de plus offre des possibilités de contrôle de qui a accès aux fichiers.

[20] http://www.google.com/google-d-s/intl/fr/tour1.html
[21] http://www.google.com/intl/fr/googlecalendar/tour.html
[22] http://www.doodle.ch/
[23] http://dl.free.fr/

Visibilité et réputation

Un nom de domaine, une adresse électronique est un élément important dans l'image de marque d'un organisme.
Utiliser pour son courrier professionnel comme adresse électronique celle d'un fournisseur gratuit, crée une ambigüité vis-à-vis des correspondants qui auront du mal à discerner si le message est professionnel ou non. En outre connaissant les problèmes juridiques posés par la distinction entre courrier professionnel et courrier privé, il ne semble pas judicieux de compliquer la situation.
Le fait de faire suivre (« forward ») son courrier vers une adresse chez un fournisseur gratuit peut conduire à de graves conséquences pour l'ensemble de l'organisme comme on l'a vu dans un cas réel. Le fournisseur avait mis en liste noire le serveur de courrier d'un établissement de recherche car il avait reçu depuis cette machine plus d'un certain nombre de messages considérés comme indésirables, ces messages provenaient d'expéditeurs extérieurs et avaient été simplement relayés. Les fournisseurs gratuits sont sans état d'âme et on les comprend car ils doivent faire fonctionner le système à moindre coût.
On ne devrait jamais utiliser un service Internet gratuit pour héberger sa messagerie électronique, a fortiori si on traite d'informations un tant soit peu sensibles, ni donner comme adresse professionnelle une adresse hébergée par un fournisseur gratuit. Cependant il peut y avoir des situations où un certain anonymat est indispensable ou tout simplement le fait de pouvoir disposer d'une adresse éphémère, jetable en quelque sorte, permet de s'inscrire à une manifestation commerciale ou de télécharger une version de démonstration d'un logiciel sans trop révéler d'informations et d'éviter du spam par la suite. Dans ce cas l'utilisation d'un service gratuit est envisageable en se limitant à ce qui est nécessaire.
Le CERTA a alerté à plusieurs reprises sur les risques présentés par l'hébergement mutualisé de sites web[24]. Pour des raisons de coût, différents sites web sont souvent regroupés sur le même serveur. La compromission de l'un d'entre eux peut entrainer celle des autres. Il est difficilement acceptable de se faire défigurer son site qui était bien développé, en respectant les bonnes pratiques, les règles de sécurité parce qu'un autre dont on ignorait jusqu'à l'existence mais qui avait le malheur de se trouver sur le même serveur, avait une faille dans une application web. Il est bien évident que chez les fournisseurs gratuits, aucune précaution ne peut être prise pour isoler les différents sites (serveurs dédiés, machines virtuelles).

Divulgation d'informations personnelles sur Internet

Google a récemment annoncé qu'il ne conservera à l'avenir (ce n'était pas encore effectif à la date de rédaction de cette note[25]) que pendant 18 à 24 mois[26], l'historique des requêtes effectuées sur son moteur de recherche. Il est bien évident que l'analyse et le recoupement de ces requêtes permettent de trouver énormément d'information sur un individu et ses centres d'intérêts.
Dans un récent avis[27] le CERTA mettait engarde contre les risques de fuites d'informations que font encourir les réseaux sociaux. Rendre publique son profil (centres d'intérêt, CV, âge, photo, lieu de résidence, etc.) ou ses contacts (amis, parents, collègues de travail, relations professionnelles, personnes fréquentant les mêmes clubs, etc. .) est tout sauf anodin. Pour faire de l'intelligence économique c'est un outil merveilleux. En croisant les informations, il

[24] http://www.certa.ssi.gouv.fr/site/CERTA-2005-INF-005/
[25] http://www.google.com/privacy.html
[26] http://googleblog.blogspot.com/2007/03/taking-steps-to-further-improve-our.html
[27] http://www.certa.ssi.gouv.fr/site/CERTA-2007-ACT-043.pdf

va être possible d'établir l'organigramme de l'organisation, déterminer les sujets de recherche.

Face à une inquiétude légitime, la loi « informatique et libertés » a été faite pour protéger l'individu du détournement de données à caractère personnel. Il est paradoxal de penser qu'avec les nouveaux usages d'Internet des inhibitions tombent et que l'individu va révéler consciemment ou non beaucoup d'informations personnelles qu'auparavant il n'aurait jamais divulguées. C'est donner des verges pour se faire battre.

Les sites communautaires ou les réseaux sociaux rendent floue la distinction entre professionnel et privé. Certaines informations font le lien entre les deux mondes. Ma liste de contacts peut contenir des amis et des collègues de travail. Dans mon profil, je peux avoir mon lieu de résidence comme mon lieu de travail.

Il ne s'agit évidemment pas d'interdire l'utilisation de ces nouveaux usages d'Internet qui peuvent être un formidable outil au service des relations humaines. De toute façon tant qu'ils restent utilisés dans le cadre de la vie privée on n'a aucune possibilité de l'interdire tout en sachant qu'un usage privé peut indirectement conduire à la fuite d'informations professionnelles. Il faut donc sensibiliser l'utilisateur aux informations qu'il rend publiques.

Annexe : Google Analytics

La société Google a racheté en 2005 la société Urchin qui vendait un service permettant de mesurer la fréquentation des serveurs. L'idée est de tracer les comportements des visiteurs afin de déterminer les améliorations à apporter au site pour en augmenter l'efficacité commerciale.
Avec ce rachat, Google a lancé son service Google Analytics[28] :
« *L'objectif de Google est de vous aider à augmenter le nombre de visiteurs sur votre site et à accroître vos ventes.*
Utilisez Google Analytics pour identifier les opérations de marketing en ligne les plus rentables et pour connaître le comportement réel des visiteurs sur votre site. Exploitez les statistiques fournies par cet outil pour apporter des améliorations à la présentation de votre site, générer un trafic ciblé et augmenter le nombre de conversions et votre chiffre d'affaires.
Inscrivez-vous maintenant. La procédure est simple et le service est gratuit ! »[29]

Les outils d'analyse de fréquentation sont très bien faits, produisent des rapports pertinents, agrémentés de beaux graphiques. Il est donc très tentant pour un exploitant de site web d'utiliser ce service d'autant plus qu'il est gratuit. Cependant il faut bien voir quelles en sont les implications.
Le principe consiste à ajouter dans les pages web du site un *javascript* qui va récupérer un certain nombre d'informations sur le visiteur (adresse IP, date et heure, page visitée auparavant, navigateur employé, etc.) et les transférer sur une machine de Google à des fins d'analyse ultérieure. Outre que la technique employée s'apparente à celle utilisée par les pirates (manipulation de cookies, affichage d'images de 1 x 1 pixel afin de les rendre invisibles, etc.) le transfert d'informations vers Google pose de nombreuses questions.
Parmi les informations transférées, il y a entre autres l'adresse IP qui est une donnée à caractère personnel[30]. Cela signifie qu'il faut respecter la loi Informatique et liberté[31] et déclarer le traitement. Celui-ci sort largement du cadre de ce qui a été déclaré par le CNRS à la CNIL en matière de gestion de traces[32]. De plus le fait que le traitement soit effectué hors Communauté européenne impose des obligations particulières.
Le risque de fuites d'informations doit être pris en considération. Les informations transmises ne sont pas nécessairement toutes anodines. Il est même possible d'utiliser Google Analytics

[28] http://www.google.com/analytics/fr-FR/

[29] http://www.google.com/analytics/fr-FR/sign_up.html

[30] Malgré deux décisions récentes de la Cour d'appel de Paris, l'adresse IP est toujours considérée par la CNIL comme une donnée à caractère personnel (http://www.cnil.fr/index.php?id=2244).

[31] Loi n° 78-17 du 6 Janvier 1978 relative à l'informatique, aux fichiers et aux libertés (http://www.cnil.fr/index.php?id=301#CHAPITRE12).
[32] Politique de gestion des traces d'utilisation des moyens informatiques et des services réseau au CNRS (https://intranet.cnrs.fr/extranet/cnrs/fsd/documents/Po_gest_traces.pdf)

pour un site web en Intranet alors que celui-ci n'est pas visible de l'extérieur ce qui va exposer des informations comme les noms des pages consultées qui peuvent permettre de reconstituer ne serait-ce que les centres d'intérêts du laboratoire.
L'utilisation de Google Analytics comme outil de mesure d'audience des sites web soulève de fortes réserves. En tout cas celle-ci ne pourrait se faire qu'après une déclaration à la CNIL. Il faut privilégier les outils locaux[33] qui vont analyser les journaux du serveur web afin d'en extraire les statistiques. Il est aussi possible d'acheter le produit Urchin pour l'héberger sur ses propres serveurs

[33] Un exemple parmi d'autres : Webalizer (http://www.mrunix.net/webalizer/).