



CASES articles

Série d'articles CASES : Web 2.0 – Les nouveaux réseaux sociaux

MySpace, Facebook, YouTube – Communautés, pièges à données et contenus dangereux

Pour plus de sécurité, adoptez les réflexes CASES !

Les données font le tour du monde, mais ne tombent pas toujours dans de bonnes mains

Femmes au foyer, artisans, managers, écoliers ou étudiants : nombreuses sont les personnes qui confient trop d'informations à l'Internet. Les sites communautaires tels que MySpace, YouTube ou FaceBook peuvent rapidement se transformer en pièges à données ou véhiculer des contenus dangereux. Des failles dans les logiciels ou encore la structure peu conviviale de certains programmes peuvent être à l'origine de ces problèmes. Peuvent également être mentionnées dans ce cadre, les connaissances lacunaires des utilisateurs en matière de failles de sécurité, et en particulier sur les failles liées aux réglages standards des applications. Il faut également préciser que les applications incitant l'utilisateur à dévoiler des données sensibles ne sont pas rares et que la méconnaissance de certains aspects juridiques peut générer de bien mauvaises surprises.

Les communautés en ligne offrent aux utilisateurs l'opportunité de faire de nouvelles connaissances, de se représenter eux-mêmes, de rester en liaison ou de reprendre contact avec des amis. Mais elles peuvent également dissimuler des pièges à données ou héberger des contenus dangereux. MySpace est une communauté en ligne bien connue. Cette plateforme permet entre autres de transmettre des données spécifiques : les utilisateurs peuvent publier des informations personnelles en rapport avec les rubriques les plus diverses. Voici quelques exemples des champs que peuvent renseigner les utilisateurs : « à propos de moi », « j'aimerais faire la connaissance de », « pôles



d'intérêt », « musique », « films », « télévision », « livres », « héros », « nom », « prénom », « sexe », « date de naissance », « profession », « pays », « code postal », « lieu de résidence », « nationalité », « mensurations », « taille », « je suis là pour du « dating » (par exemple), « état civil », « religion », « enfants », « nom de l'école », « formation » et « revenu ».

Divulgarion de données sensibles par les utilisateurs

« La quantité d'informations divulguées sur eux-mêmes par les utilisateurs d'applications Web 2.0 est vraiment surprenante. Ceux-ci devraient pourtant bien réfléchir aux données qu'ils souhaitent réellement communiquer. Quelles sont les informations vraiment judicieuses et quelles sont

celles complètement inutiles ? Parfois, l'on a l'impression que les applications Web 2.0 font tout pour pousser l'utilisateur à révéler beaucoup plus de données que nécessaire, mais la communication de ces informations reste bien sûr facultative », explique François Thill, du portail de sécurité Internet luxembourgeois CASES.

Le besoin d'autoreprésentation incite de nombreux utilisateurs, et en particulier des adolescents, à s'inscrire sur des plateformes Web 2.0 et à y divulguer des informations privées. Pourtant, la simple vérification sur l'Internet d'un candidat à un poste par le bureau du personnel d'une société permet de mieux comprendre que toute information divulguée à la légère peut rapidement se transformer en obstacle insurmontable : une pose jugée déplacée sur une photo prise à l'occasion d'une fête ou pendant les

vacances peut suffire pour se voir notifier un refus.

Les manchettes de plus en plus fréquentes relatant des cas d'usurpation d'identité par des tiers malveillants sont également sans équivoque. Les adolescents et les enfants, mais également les adultes, doivent décider eux-mêmes quelles données personnelles ils peuvent divulguer sans danger. Et ce n'est pas toujours chose facile ! Il convient également de se souvenir que l'Internet a la mémoire longue : des informations divulguées dix ans plus tôt peuvent subitement devenir très embarrassantes. Les dispositions sur la protection des données de certaines applications peuvent également s'avérer très utiles. La lecture de la très explicite politique de confidentialité de MySpace permet par exemple aux utilisateurs de connaître les aspects à prendre en considération. Malheureusement, ces dispositions ne sont bien souvent pas lues par les utilisateurs avant leur inscription et il suffit de poser la question à ses propres enfants, à ses parents, des amis, collègues de travail ou voisins pour s'en rendre compte.

Le traitement de « données se rapportant à des personnes » est soumis à des dispositions légales. Sont considérées comme des données se rapportant à une personne toutes celles qui permettent de l'identifier. Ainsi, le nom, des photos, l'adresse, le numéro de téléphone, l'adresse e-mail, le matricule ou l'adresse IP en font de toute évidence partie. Mais les informations sensibles suivantes sont également considérées comme des données se rapportant à une personne : origine ethnique, opinion politique, convictions religieuses ou philosophiques, appartenance à un syndicat, santé ou encore sexualité.

Il convient d'éviter de divulguer ces informations sur l'Internet et ce, même si les applications Web 2.0 proposent des fonctions de protection permettant de restreindre les droits d'accès de tiers par exemple. Des failles dans ces logiciels permettent en effet souvent aux hackers de contourner ce genre de fonction de protection. De plus, certains utilisateurs ne sont pas toujours ce qu'ils prétendent être et des amis virtuels peuvent en fait se

révéler des individus bien malintentionnés.

Frontières nationales et lois

La toile ne connaît pas les frontières – la justice, oui ! Les portails Web 2.0 peuvent dissimuler des risques pour les consommateurs et les utilisateurs, comme le démontre l'exemple du portail vidéo YouTube.

YouTube, tout comme d'autres portails vidéo, est soumis à des conditions d'utilisation très claires : les contenus pornographiques, illégaux ou violents y sont par exemple interdits, et les droits de la personne ainsi que les droits d'auteur doivent être respectés.

Or, ce sont les lois des États-Unis qui s'appliquent pour YouTube et cela génère un hiatus profond entre les conditions d'utilisation telles qu'elles sont édictées et la pratique. La « *Beschwerdestelle für jugendgefährdende Inhalte im Internet* » allemande (centre de réclamations et de plaintes contre les contenus dangereux pour la jeunesse sur Internet) en a par exemple fait l'expérience à l'été 2007. Des contenus d'extrême droite avaient alors été publiés sur le portail vidéo et des utilisateurs les avaient signalés à cet organisme. Le centre de réclamation et de plainte allemand ne dispose toutefois d'aucun recours légal pour imposer le retrait de tels contenus, le droit applicable étant celui des États-Unis. Selon les indications de l'organisme allemand, la société YouTube n'a même pas jugé bon de réagir aux messages qui lui ont été adressés à cette occasion.

Les portails vidéo ne disposent généralement pas de systèmes de vérification de l'âge des utilisateurs lorsqu'ils s'inscrivent, ce qui signifie que les enfants et les adolescents peuvent également accéder à ce genre de contenu.

Les États-Unis réagissent toutefois beaucoup plus rapidement lorsqu'il s'agit d'effacer des contenus de propagande terroriste, ces derniers ayant connu une augmentation significative. Mais une fois de plus, les utilisateurs doivent d'abord signaler les contenus en question, car aucun contrôle n'est

prévu du côté des portails avant la mise en ligne des contenus vidéo.

Force est de constater que les adolescents peuvent être exposés très facilement à des contenus dangereux pouvant altérer leur développement sur les portails vidéo. Malgré leur interdiction, des vidéos pornographiques ou de mobbing peuvent y être visionnées, aucune mesure de protection efficace n'y étant appliquée.

Les personnes mettant en ligne des vidéos peuvent d'ailleurs également avoir de mauvaises surprises. L'industrie de la musique américaine, par le biais de son lobby RIAA, a ainsi obtenu le retrait de vidéos de karaoké par décret de justice en 2007. Les personnes qui chantent leur chanson préférée sur la musique originale du morceau au cours de joyeuses soirées entre amis ou de fêtes peuvent se retrouver assignées en justice par l'industrie du disque américaine. La musique utilisée sur ces vidéos est en effet protégée par des droits d'auteur. L'industrie du disque est dans son bon droit et la personne ayant mis en ligne la vidéo contrevient à l'interdiction de diffusion publique. Les droits de diffusion sont en effet exclusivement réservés à l'éditeur, à l'auteur ou au compositeur. Dans ce genre de plainte, les frais d'avocat sont également à la charge de la personne ayant mis la vidéo en ligne. En outre, la partie lésée est en droit de demander des dommages et intérêts.

Pièges à données

Plus de 20 000 utilisateurs se sont inscrits sur le réseau luxembourgeois de la communauté en ligne Facebook. Pour de nombreux adultes, cette application permet de retrouver des camarades d'école, voire même du jardin d'enfants. Les réglages standard de cette application et les possibilités d'adaptation personnalisée qu'elle offre permettent de démontrer à quel point il est facile pour l'utilisateur de devenir la victime de pièges à données.

Lors de l'inscription initiale, les réglages standards sont déjà paramétrés afin que les amis et les autres membres des réseaux puissent visualiser les données personnelles de l'utilisateur. Dès que la personne de-

vient membre d'un réseau, tous les utilisateurs de ce même réseau ont donc accès à ses données. Pour le réseau luxembourgeois de Facebook, cela signifie par exemple que plus de 20 000 utilisateurs auront automatiquement accès aux données privées de la personne. Liste des amis, profil personnel, photos ou vidéos – tout devient largement accessible. Il est fortement recommandé à l'utilisateur d'ajuster le niveau de sécurité des réglages et, par exemple, d'interdire l'accès des réseaux à ses données.

Mais à peine ce premier piège à données, somme toute assez simple, est-il déjoué à l'aide d'ajustements judicieux, que le prochain piège guette l'utilisateur. Imaginons que l'utilisateur ait modifié les réglages standards dès le début, de manière à interdire l'accès des réseaux à ses données personnelles. Cet utilisateur est donc prudent. Mais que se passe-t-il lorsqu'il rejoint un réseau, par exemple celui du Luxembourg ? Un simple clic suffit à cet effet et l'application Facebook modifie alors automatiquement les réglages effectués manuellement auparavant par l'utilisateur. Le réglage de l'utilisateur interdisant aux ré-

seaux d'accéder à ses données est modifié automatiquement : les réseaux auxquels appartient l'utilisateur ont maintenant accès à ses données. Le réseau luxembourgeois obtient donc automatiquement l'accès aux données de cet utilisateur. Ses informations personnelles deviennent ainsi accessibles à plus de 20 000 utilisateurs. L'utilisateur doit donc veiller à vérifier les réglages du niveau de sécurité chaque fois qu'il ajoute des réseaux. Les manipulations nécessaires doivent être effectuées de nouveau, l'accès des réseaux aux données correspondantes doit une fois de plus être interdit manuellement.

Les pièges à données peuvent être astucieux. L'équipe CASES a pu vérifier cet état de fait grâce à l'aide de deux personnes test : deux adultes sensibilisés au problème, mais n'ayant jamais utilisé Facebook auparavant. Ce test a permis de constater qu'à l'issue d'une période d'utilisation de l'application de quatre heures, les sujets n'étaient pas encore en mesure de détecter tous les pièges à données et qu'ils n'avaient pas découvert toutes les modifications de réglage nécessaires. La divulgation de données

Conseil de sécurité : les bons réglages pour Facebook

CASES a rédigé un guide présentant les pièges à données possibles ainsi que les fonctions de protection propres à l'application Facebook. Ce guide décrit divers pièges à données qui, malgré une apparence changeant régulièrement, sont toujours présents dans cette application. Ce document est disponible sur le site www.cases.lu. Il est recommandé aux parents de s'intéresser en particulier aux applications Web 2.0 qu'utilisent leurs enfants. Afin d'obtenir une meilleure vision d'ensemble, il peut être judicieux de créer un profil test dans ces applications.

sensibles était donc toujours possible. Il n'est guère probable que des enfants et des adolescents, ou toute autre personne n'ayant pas été sensibilisée à ce problème, puissent obtenir de meilleurs résultats.

Retrouvez les dossiers, fiches thématiques alertes et actualités sur:

www.cases.lu