MINISTÈRE DE L'ÉDUCATION NATIONALE, DE L'ENSEIGNEMENT SUPÉRIEUR ET DE LA RECHERCHE

INFORMATION AUX RSSI

LE DANGER DES APPLICATIONS DE MESSAGERIE MASQUANT L'USAGE D'UN CLOUD NON MAITRISE

HFDS/SPDS/FSSI 04 avril 2016

Le danger des applications de messagerie masquant l'usage d'un cloud non maitrisé

De nombreuses applications sont disponibles, en particulier pour les smartphones, pour accéder à sa messagerie. Certaines sont natives dans les OS, d'autres peuvent être téléchargées, souvent gratuitement, sur les AppStores d'Apple, d'Android ou ailleurs.

L'utilisation de ces applications nécessite que l'utilisateur renseigne ses informations de comptes, identifiant et mot de passe, afin de pouvoir se connecter et récupérer ses messages.

Le fait de renseigner ces informations est une prise de risque que l'on ne peut pas éviter, mais qui reste maitrisée tant que les messages sont récupérés par l'appareil et que les identifiants restent enregistrés localement.

Cependant, certaines applications semblent fonctionner sur les terminaux mais ne sont en fait que des relais d'affichage. Les identifiants sont transmis à un serveur tiers qui se charge de récupérer les messages.

Un disfonctionnement avec l'application MyMail, constaté sur les infrastructures de Renater, a mis en avant ces problématiques. (L'analyse est présentée ci-après)

Enjeux de sécurité

Ces solutions n'offrent aucune garantie:

- L'utilisateur donne à un tiers inconnu l'accès à l'ensemble de ses messageries.
- L'utilisateur n'a aucune connaissance de l'archivage et l'usage possible de ses messages.
- L'utilisateur n'a aucune maitrise de l'utilisation de ses comptes (ex : envoi de SPAM).
- L'utilisateur ne sait pas où sont les serveurs ni à quelles réglementations ils sont soumis.
- Même si le flux avec la messagerie était chiffré, dans certains fonctionnements, il n'y a plus aucune garantie entre le serveur tiers et le terminal.
- En cas de désinstallation de l'application, le serveur continue dans certains cas à récupérer les messages.

Benoît MOREAU – Fonctionnaire de sécurité des systèmes d'information
99, rue de Grenelle 75357 Paris 07 SP 01 55 55 84 85
benoit.moreau@education.gouv.fr benoit.moreau@recherche.gouv.fr

Analyse du disfonctionnement par Renater

Suite à la détection sur la messagerie PARTAGE de RENATER d'un trafic important en volume et en nombre de sessions avec des serveurs dans le domaine MY.COM, un filtrage a du être mis en place et une analyse a été faite pour comprendre la raison de ce trafic. Il s'est avéré qu'il était dû à l'utilisation, dans certains établissements, de l'utilisation de l'application MyMail.

Cette application, très bien notée par ailleurs, et accessible sur les AppStores d'Apple et de Google, ressemble à une application comme il y en a beaucoup pour accéder à sa messagerie.

Après avoir installé l'application et configuré le compte de messagerie de son établissement, l'utilisateur peut l'utiliser pour lire ses messages.

Or cette application n'est pas un client lourd de messagerie.

Les informations de comptes sont transmises à des serveurs basés aux Pays-Bas, dans le domaine MY.COM, domaine appartenant à MAIL.RU, à priori un service de messagerie russe...

Ce sont ces serveurs qui vont se connecter en IMAP sur le serveur de messagerie, avec accès illimité aux boites aux lettres de l'utilisateur.

L'application, elle, va se connecter en HTTPS sur ces serveurs pour présenter les messages à l'utilisateur.

On voit là que le niveau de risque est bien plus important que pour des clients de messagerie classique.

Recommandations

Dans un contexte professionnel, il convient d'utiliser la messagerie proposée par les services informatiques. Si le choix revient à l'utilisateur, il est recommandé d'utiliser les applications de messagerie fournies sur les OS officiels ou ayant fait l'objet d'une analyse de risque ou à minima de fonctionnement.

Benoît MOREAU – Fonctionnaire de sécurité des systèmes d'information
99, rue de Grenelle 75357 Paris 07 SP 01 55 55 84 85
benoit.moreau@education.gouv.fr benoit.moreau@recherche.gouv.fr