5 conseils pour sécuriser Microsoft Teams

Le recours massif au télétravail depuis le 16 mars dernier a conduit de nombreuses entreprises à se tourner vers des solutions de collaboration modernes telles Microsoft Teams, désormais proposé avec la plupart des offres Office 365. Mais une bonne compréhension de ce dernier est essentielle pour éviter la fuite accidentelle d'informations.

Microsoft Teams est une solution de travail collaboratif parfaitement adaptée au télétravail. Avec Teams, des équipes distantes peuvent collaborer autour de plusieurs canaux de discussion, partager des fichiers en interne comme en externe, et même éditer ces derniers de manière collaborative directement dans l'interface Teams.

Du point de vue du responsable de la sécurité du système d'information (le RSSI), toutefois, il est vital de bien comprendre comment Microsoft Teams fonctionne et notamment comment cette solution s'appuie sur l'infrastructure existante. Car derrière Teams, l'on retrouve les OneDrive et les Sharepoint traditionnels. En définitive, Teams peut donc être vu comme un nouveau frontend pour les services de partage de fichiers habituels. Il propose aux collaborateurs de nouvelles manières de diffuser l'information mdash; en particulier au sein des groupes de discussion qui peuvent intégrer des externes mdash; et il est important d'être en mesure d'en contrôler la diffusion !

Facilité de partage

Les utilisateurs de Teams sont encouragés à partager des documents, et l'interface de la solution reflète parfaitement cette philosophie : il est ainsi trivial d'ajouter un document durant une conversation de groupe, et l'ensemble des fichiers ainsi partagés se retrouve classé par format dans des onglets aisément accessibles. Derrière tout ça, les documents sont stockés sur une instance Sharepoint et accessibles aux participants du canal de discussion en question.

Or si la maîtrise des droits Sharepoint est généralement bien comprise par les administrateurs, l'irruption de Teams et des comptes dits « invités » peut changer la donne. Car l'administrateur qui aurait activé un peu précipitamment l'accès « invités » sur son offre Teams ignore peut-être que chaque invité est en réalité un nouvel utilisateur sur son annuaire Active Directory, et que ce dernier peut être convié à rejoindre potentiellement n'importe quel canal de discussion. Et si durant le fil de la discussion des documents internes sont partagés, ceux-ci demeureront disponibles pour tous les participants mdash; y compris les invités mdash; tant qu'ils ont accès au canal.

Ce scénario est bien entendu parfaitement légitime et il fait même partie de la force de la solution. Pour le RSSI, toutefois, cela signifie qu'il doit garder de la visibilité non seulement sur les contenus disponibles sur ses Sharepoint, mais désormais également sur la manière dont ceux-ci peuvent être accédés via les nouveaux canaux de discussion Teams ouverts aux invités (cette fonctionnalité n'est apparue qu'en novembre 2019, elle est donc très récente et pas toujours bien comprise).

Voici les cinq règles essentielles d'une bonne sécurisation des partages avec Microsoft Teams :

1. Implémenter le contrôle d'accès multifacteurs

Considéré comme l'une des manières les plus efficaces de réduire l'impact du vol d'identifiants, dans un contexte Teams le MFA permet de garantir à minima que les invités seront bien seuls à se connecter, même s'ils se font voler leurs identifiants (et c'est d'autant plus important que le RSSI ne peut contrôler comment ces derniers seront protégés).

2. Classifier les documents sur Sharepoint Online

Puisque tout document partagé dans le cadre d'une discussion Teams finira stocké sur Sharepoint Online, ce dernier est l'endroit idéal ou traquer les informations sensibles n'auraient pas à s'y trouver, y compris lorsqu'elles proviennent d'un partage dans une discussion Teams.

3. Empêcher le téléchargement sur des équipements non contrôlés

Tout document partagé dans le cadre d'une discussion Teams n'a pas forcément besoin d'être téléchargé par les participants extérieurs, notamment parce que Teams propose déjà leur édition directement depuis son interface.Si les besoins métiers le permettent, il peut être utile de limiter le téléchargement des fichiers aux seuls terminaux gérés par la DSI (internes, donc).

4. Contrôler régulièrement les utilisateurs invités

Le nombre d'utilisateurs extérieurs (« invités ») qu'il est possible d'activer dépend de du niveau de licence Azure AD (voirhttps://docs.microsoft.com/fr-fr/azure/active-directory/b2b/licensing-guidance). Leur nombre est donc limité et il est bon d'auditer régulièrement les instances Azure AD afin de surveiller combien de comptes invités sont créés, de désactiver les plus anciens et peut-être détecter des anomalies, ou identifier des utilisateurs internes qui abuseraient de cette fonctionnalité à des fins personnelles.

5. Auditer les partages SharePoint « invités »

Il s'agit là d'une bonne pratique de l'administration SharePoint classique, mais elle est tout aussi importante dans un contexte Teams :auditer en continu les documents partagés publiquement. Dans SharePoint, cela passe habituellement par des liens de partage configurés pour être accessible à tout le monde. Dans Teams, cela passera désormais aussi par des documents attribués à des utilisateurs « invités » spécifiques. Il sera donc nécessaire de faire le lien entre tel utilisateur invité, le canal de discussion auquel il appartient et les documents qui lui ont été partagés, afin de s'assurer que parmi ces derniers ne figurent pas d'information sensible à laquelle un externe ne devrait pas avoir accès.

En définitive, Microsoft Teams offre à ses utilisateurs de nouvelles façons efficaces de consommer et de partager l'information de l'entreprise, y compris avec des externes. Il est impératif pour le RSSI de bien comprendre comment fonctionnent ces nouveaux partages et de les intégrer à sa stratégie de protection de l'information sur SharePoint.