Microsoft Teams rouvre le débat environnement ouvert vs. sécurité

Après l'ascension irrésistible de Slack, Teams a connu, à son tour, un succès fulgurant. En novembre 2019, Microsoft annonçait 20 millions d'utilisateurs quotidiens, dont 7 millions acquis juste sur les quatre mois précédents.

Teams est un outil simple à utiliser qui transforme la manière dont les équipes communiquent, collaborent et partagent des informations. L'intégration avancée des GIFs, avec une bibliothèque mise à jour en permanence, illustre bien la volonté de Microsoft de se montrer ouvert et inclusif de tous les nouveaux usages, même les plus inattendus.

Dans les faits, Teams apporte une nouvelle manière de travailler et une productivité globale accrue pour les entreprises, mais également son lot de vulnérabilités. Il est important pour les administrateurs et responsables IT de connaître ces risques et la manière de s'en prémunir.

Une politique d'accès par défaut inhabituellement souple

Microsoft a voulu favoriser une adoption massive et, pour y parvenir, la compatibilité et l'intégration avec un vaste écosystème applicatif sont importantes.

L'intégration d'applications tierces par les utilisateurs directement dans les groupes de discussion est l'une des fonctions phares de Teams. Par exemple, il est possible d'ajouter des bots, de faire des sondages rapides ou de connecter des services de stockage cloud.

Par défaut, il est possible pour les utilisateurs de télécharger n'importe quelles applications dans leur environnement, souvent en communiquant simplement leur adresse email professionnelle. Cet accès inhabituellement peu restrictif a permis à Microsoft de conquérir des parts de marchés colossales en très peu de temps.

D'un point de vue commercial c'est une stratégie indiscutable. Du point de vue de la sécurité des infrastructures, c'est, au contraire, un parti pris qui pose question. Le fait est que la plupart des administrateurs réseaux et systèmes ignorent que cet accès est activé par défaut.

Certaines des applications tierces disponibles dans l'app store de Team peuvent s'avérer malveillantes ou tout simplement vulnérables. C'est un risque conséquent dans la mesure où de nombreuses informations sensibles peuvent transiter dans un canal Teams. Des données clients, une roadmap produit ou des schémas IP pour ne donner que trois exemples marquants.

Microsoft a mis en place des outils pour vérifier les applications et controler leur publication sur le store mais il n'en demeure pas moins qu'il est possible que certaines applications présentent encore des défauts de sécurité. Il existe de nombreux exemples sur tous les app stores, y compris les plus réputés.

Comment protéger votre organisation contre les applications Microsoft Teams vulnérables

Microsoft n'a pas rendu la tâche évidente mais pas impossible pour autant. Les administrateurs peuvent travailler sur deux axes principaux pour renforcer les politiques d'autorisation pour les applications Teams:

– En tant qu'administrateur, les politiques d'autorisation permettent de gérer au niveau de l'entreprise les applications disponibles sur Microsoft Teams. Il est ainsi possible d'autoriser ou de bloquer toutes les applications ou des applications spécifiques publiées par Microsoft, des tiers et même par votre entreprise. Lorsqu'une application est bloquée, les utilisateurs ne peuvent pas l'installer à partir de l'app store Teams.

– La gestion des politiques d'autorisation des applications dans le centre d'administration de Microsoft Teams permet d'appliquer des paramètres à l'échelle de l'entreprise, utiliser la politique globale (par défaut à l'échelle de l'entreprise), et créer et attribuer des politiques personnalisées au niveau individuel ou d'un groupe est une procédure simple qui permet d'aboutir rapidement à une plus grande sécurité.

Pour éviter que Microsoft Teams expose les données d'une entreprise, il est essentiel que cette dernière ait connaissance de quelles sont les applications qu'elle souhaite autoriser et lesquelles elle souhaite bloquer et à quel niveau. Il est impératif pour les administrateurs informatiques de prendre en compte cet aspect de Microsoft Teams pour maîtriser la sécurité de leur entreprise.