Cartographie des risques Office 365

SaaS

- **RC01** ●●● Vol et Usurpation d'identité
- **RC02** ●●● Non maîtrise de la réversibilité
- **RC03** ●●○ Mauvaise gestion des identités et des accès
- **RC04** ●●○ Fuite de données incontrôlée
- **RC05** ●●○ Modification majeure des fonctionnalités
- **RC06** ●●○ Saturation réseau à la suite d'une évolution des usages
- **RC07** ●○○ Altération / perte de données
- **RC08** ●○○ Indisponibilité du service

Collaboration

Teams OneDrive Sharepoint

- **RS01** ●●● Fuite via des partages trop permissifs
- **RS02** ●●● Mauvaise gestion des groupes O365
- **RS03** ●●○ Mauvaise gestion des permissions sur un partage
- **RS04** ●●○ Fuite via le partage d'un lien anonyme
- **RS05** ●●○ Diffusion de fichiers malfaisants
- **RS06** ●○○ Usage non conforme à la charte

Communication

Outlook Yammer Teams

- **RM01** ●●● Redirection malveillante de messages
- **RM02** ●●● Ingénierie sociale (phishing) ciblée O365
- **RM03** ●●● Délégation non maîtrisée par l'utilisateur
- **RM04** ●●○ Usurpation de domaine messagerie
- **RM05** ●●● Fuite de données via un service tiers
- **RM06** ●●○ Utilisation d'anciens protocoles (imap, pop3)
- **RM07** ●○○ Mauvaise configuration de la rétention

Bureautique

Excel Notes PowerPoint Word

- **RP01** ●●○ Exécution de codes malveillants
- **RP02** ●○○ Incompatibilité à la suite d'une mise à jour

Développement

PowerApps PowerBi Flow Forms

- **RD01** ●●● Secrets d'authentification non protégés
- **RD02** ●●● Mauvaise gestion des droits
- **RD03** ●●● Mauvais paramétrage Oauth
- **RD04** ●○○ Fuite par détournement de fonctionnalité
- **RD05** ●○○ Interface mal contrôlée avec une application

Gestion du tenant

Office 365

- **RA01** ●●● Mauvaise gestion des arrivées/départs
- **RA02** ●●● Mauvaise gouvernance des services
- **RA03** ●●● Perte de traçabilité des actions des administrateurs
- **RA04** ●●● Non ségrégation de l'administration
- **RA05** ●●● Absence de surveillance des comptes à privilèges
- **RA06** ●●○ Non adéquation de l'équipe d'administration
- **RA07** ●●○ Administration depuis un appareil compromis
- **RA08** ●●○ Erreur / méconnaissance de l'administrateur
- **RA09** ●●○ Fédération identités mal maîtrisée (Azure AD)
- **RA10** ●●○ Mauvaise gestion des clés du tenant par l'organisation
- **RA11** ●●○ Non maîtrise des montées de version des services
- **RA12** ●●○ Mauvaise gestion des droits des invités

Lois

- **RG01** ●●● Risque financier / maîtrise des licences
- **RG02** ●○○ Non-conformité réglementaire
- **RG03** ●○○ Difficulté à répondre à une réquisition judiciaire

Appareils

- **RE01** ●●● Usage depuis un appareil compromis
- **RE02** ●●○ Usage depuis un appareil perdu/volé
- **RE03** ●●○ Usage depuis un appareil non maîtrisé

Niveau de risque

- ●●● Probable/conséquences importantes
- ●●○ Possible/conséquences moyennes
- ●○○ Peu probable/ conséquences limitées

CLUSIF

Cette infographie est issue d'un groupe de travail du CLUSIF (www.clusif.fr). Elle présente les menaces et vulnérabilités d'Office 365 mais ne peut être exhaustive.

version Juillet 2019