LES DOSSIERS TECHNIQUES

Office 365 et sécurité

Décembre 2020

CLUSIF

Table des matières

Table des illustrations

Remerciements

Le Clusif tient à mettre ici à l'honneur les personnes qui ont rendu possible la réalisation de ce document, tout particulièrement :

Le responsable du groupe de travail :

Jean-Marc	**BOURSAT**	*Total*

Les contributeurs :

François	**FÉVRIER**	*Astek*
Henri	**CODRON**	*Schindler*
Gilles	**D'ARPA**	*Rohde & Schwarz Cybersecurité*
Lionel	**DESCHAMPS**	*Sagemcom*
Richard	**DHIEUX**	*Interiale Mutuelle*
Jean-Noël	**GELIS**	*Nutrition & Santé*
Jean-Yves	**GRASSET**	*Microsoft France*
Pierre	**GROSBOIS**	*AG2R La Mondiale*
Michael	**JACQUES**	*Inventiva*
Thibault	**JOUBERT**	*Wavestone*
Arnaud	**JUMELET**	*Microsoft France*
Yann	**KERNANEC**	*Eliade*
Gérard	**LEYMARIE**	*Elior*
Ali	**MOKHTARI**	*Rohde & Schwarz Cybersécurité*
Fabrice	**POLLART**	*Maisons et Cités*
Daniel	**REZLAN**	*Idecsi*

Le Clusif remercie les autres membres du groupe de travail ayant participé aux discussions préalables à l'élaboration de ce document.

Le Clusif remercie également les adhérents ayant participé à la relecture.

I. Introduction

I.1. Description du sujet

L'évolution de la technologie et des offres pousse les organisations à revoir leur stratégie liée à l'espace de travail numérique *(digital workplace)*. Cette révision concerne avant tout la messagerie, qui se veut de plus en plus accessible, sur tout type d'appareil avec un haut niveau de disponibilité.

Ce besoin remet en cause les systèmes de messagerie hébergés en interne qui nécessitent beaucoup d'efforts pour les maintenir et les sécuriser. Le besoin de collaboration est un autre vecteur de changement. Le partage de documents ou la coédition de documents nécessite des outils et des infrastructures modernes et accessibles par tous les acteurs, y compris parfois par les fournisseurs ou les partenaires de l'organisation.

Cette évolution a poussé ou pousse encore les organisations à considérer les offres SaaS (Software as a Service) comme une alternative aux anciennes solutions internes. Ce mouvement concerne tous les types d'organisations, des TPE aux multinationales. Microsoft et Google sont les deux principaux acteurs et les seuls à proposer des suites logicielles intégrées. En parallèle, d'autres acteurs du cloud proposent des offres qui couvrent partiellement les besoins cités plus haut.

Ce document n'a pas vocation à éclairer le lecteur sur le choix de sa solution cloud – un autre groupe de travail du Clusif traite de ce sujet – mais il se focalise sur une des solutions, *a priori* la plus utilisée ou étudiée par les membres du Clusif, qui est la solution de Microsoft : Office 365.

Microsoft Office 365 est une suite logicielle riche qui évolue rapidement, avec un modèle de licence complexe. Ce document se veut indépendant et nous ne rentrerons pas dans le détail de ce modèle. Au contraire, ce document apporte un éclairage sur la sécurité à mettre en œuvre, quels que soient le modèle de licences ou la solution envisagée, de Microsoft ou d'un tiers.

I.2. À qui s'adresse ce document ?

Ce document s'adresse aux RSSI dont l'organisation a fait le choix Office 365 ou s'apprête à le faire. Il s'adresse aussi aux DSI et à leurs équipes, en particulier celles en charge de l'espace de travail (messagerie, solutions de partage de documents, etc.).

Il s'adresse également à toutes les personnes souhaitant mieux comprendre les enjeux sécurité d'Office 365 et les mesures à implémenter pour maîtriser les risques et, par conséquent, utiliser cette suite logicielle en ayant conscience des mauvaises pratiques à éviter.

Un glossaire est disponible en fin de document.

I.3. Objectifs du document

Ce document a pour objectif d'apporter un éclairage cybersécurité à l'usage d'Office 365 dans un cadre professionnel. Il donne des réponses aux questions suivantes.

- **Quels sont les principaux composants d'Office 365 ?**

Le chapitre II présente Office 365 pour aider le lecteur à appréhender la suite du document. Ce chapitre donne les liens à suivre par les lecteurs désireux d'en savoir plus.

- **Quels sont les risques associés à l'usage d'Office 365 ?**

Le chapitre III rappelle les risques liés à l'utilisation d'une solution cloud SaaS et présente les risques spécifiques à Office 365, pour résumer :

- **les risques liés aux appareils utilisés ;**
- **les risques liés à la collaboration et à la communication ;**
- **les risques liés au développement d'applications ;**
- **les risques liés à l'évolution des produits bureautiques ;**
- **les risques liés à la gestion du locataire (tenant).**

Ce chapitre aborde également les aspects réglementaires liés à la solution, même si le biais « conformité » n'est pas l'objectif de ce document.

- **Quelles sont les bonnes pratiques et les mesures de sécurité à adopter ?**

Le chapitre IV décrit les principales mesures de sécurité, et en particulier les bonnes pratiques à adopter pour utiliser Office 365 en conscience.

Ce chapitre se focalise sur les mesures de sécurité proposées par Microsoft ou d'autres éditeurs.

Le groupe de travail est parfaitement conscient que l'implémentation desdites mesures est dépendante d'une part du contexte des organisations, comme leur secteur d'activité, la nature des données manipulées et, d'autre part, des nombreuses contraintes spécifiques que doit gérer chaque RSSI qui peuvent être d'ordre budgétaire, organisationnel, technique, voire dépendantes des directives de la Direction générale. Le groupe de travail a également voulu prendre en compte les niveaux de maturité de sécurité hétérogènes qui existent dans les organisations.

C'est pourquoi, avec l'ambition de fournir des mesures s'adaptant à tous les contextes, le groupe de travail ne présente pas un catalogue de solutions mais, bien au contraire, s'attache à proposer un éventail de mesures de sécurité à appliquer dès que possible structuré en 6 points principaux :

- mesures de gouvernance ;
- mesures d'hygiène et bonnes pratiques ;
- mesures de gestion des identités et des accès à Office 365 ;
- mesures de protection de l'information stockée dans Office 365 ;
- mesures de détection des événements sécurité Office 365 ;
- mesures de protection contre les risques réglementaires.

I.4. Avis important : complexité & analyse de risques

L'objectif du document n'est pas de donner les arguments pour décider ou non du déploiement d'Office 365, mais bien de fournir aux organisations ayant déjà choisi de déployer Office 365 une **vision sécurité basée sur une approche d'analyse de risques**.

L'approche peut apparaître **complexe** à la fois par la taille du document, le nombre de risques et de mesures. Mais **chaque organisation ne sera pas obligatoirement concernée par**

l'ensemble des risques. C'est par sa propre analyse de risques qu'elle devra déterminer ceux qui la concernent en priorité.

De plus, une grande partie des mesures s'appuient sur les bonnes pratiques décrites par l'éditeur, qu'il s'agisse par exemple de paramétrages des services, de mise en œuvre de fonctionnalités additionnelles de protection des données (par exemple chiffrement additionnel), de l'accès conditionnel ou de renforcement de l'authentification par plusieurs facteurs.

D'autres mesures organisationnelles, par exemple une gestion stricte des identités ou une formation des utilisateurs, ne sont pas directement liées au service Office 365, mais participent pleinement au renforcement de la sécurité.

II. Comprendre Office 365

Office 365 est une offre cloud SaaS hébergée par Microsoft.

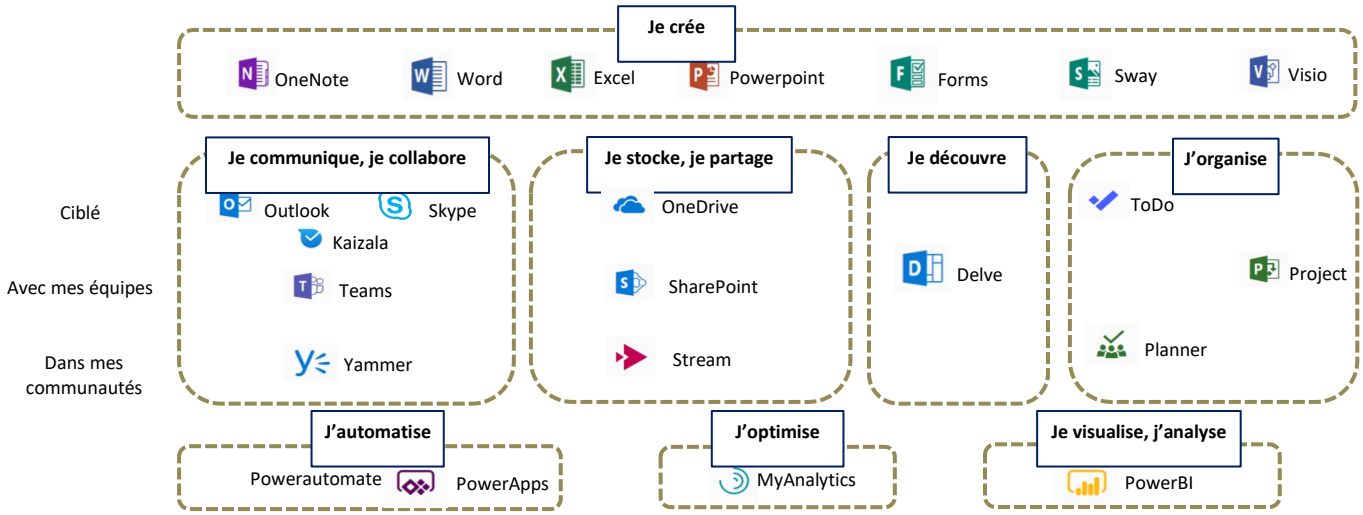
Elle a pour vocation de répondre à différents besoins de collaboration et de communication modernes, comme la messagerie, la mobilité, le réseau social, la collaboration documentaire ou de données, la messagerie instantanée, etc. Office 365 est bâtie sur des piliers importants comme la sécurité, la transparence, la localisation des données ou la richesse d'administration.

La solution est conçue pour s'adapter aux besoins des organisations, de petite, moyenne ou grande taille.

II.1. Services de collaboration d'Office 365

Office 365 offre des méthodes de collaboration modernes, basées sur un accès où que vous soyez, en mobilité ou non, que ce soit depuis un poste de travail (PC ou Mac), une tablette ou un smartphone (Android, iOS ou Windows), avec une expérience utilisateur unifiée entre les services.

Les services et les données sont accessibles soit 100 % en ligne à travers un navigateur, soit *via* un périphérique mobile ou encore *via* un client lourd, ainsi qu'avec un mode déconnecté, sans compromis de productivité.



Les différentes briques et fonctionnalités d'Office 365

Les modules « Je découvre » et « J'organise » ne sont pas couverts spécifiquement dans ce document.

- **Suite bureautique (Word, Excel, PowerPoint, OneNote) :** client lourd (Microsoft 365 Apps), client léger (Office Online) et applications mobiles (Microsoft Office pour iOS ou Android).
- **Exchange Online :** solution de messagerie (messages, calendrier, contacts, tâches).
- **SharePoint Online :** stockage et gestion de contenu documentaire.
- **OneDrive for Business :** stockage propre à un utilisateur de documents.

- **Delve :** moteur de recherche intelligent intégré à Office 365, basé sur Microsoft Graph.
- **Microsoft Teams :** outil de réunion en visioconférence et de collaboration qui agrège les services Office 365.
- **Skype Entreprise :** messagerie instantanée, webconférence, téléphonie (fin au 31/07/2021 pour la version Online – remplacée par Teams).
- **Stream :** portail vidéo d'entreprise.
- **Power Platform (Power BI, Power Automate – ex-Flow – et Power Apps) :** visualisation de données, automatisation de processus et création d'applications sans ligne de code ?
- **Planner :** gestion de tâches d'équipes.
- **Yammer :** réseau social d'entreprise.
- **Forms :** création de sondages et d'enquêtes.
- **Sway :** création de contenus interactifs.
- **Workplace Analytics et My Analytics :** outils d'analyse pour les collaborateurs.

Chacun de ces services peut être utilisé de façon indépendante des autres et déployé à des rythmes différents par les organisations, bien que certains soient fortement liés comme Teams et OneDrive pour le partage de documents dans le cas de conversations entre deux personnes.

II.2. Fonctions de sécurité pour Office 365

Office 365 ne doit pas être confondu avec Microsoft 365 Entreprise, appellation regroupant Office 365, Windows 10 et Enterprise Mobility and Security (solutions de sécurité et de mobilité).

Microsoft intègre dans Office 365 des fonctions de sécurité, des paramètres pour permettre aux entités de définir leur politique de sécurité liée à Office 365 et des consoles pour visualiser sa posture de sécurité ou pour détecter et répondre à des comportements anormaux. Ces outils complètent ceux propres à Azure (Office 365 étant une des briques d'un locataire [tenant] Azure). Le tableau ci-dessous donne une première vision de ces fonctions de sécurité existantes lors de la rédaction de ce document, sachant que des évolutions régulières sont apportées par Microsoft pour enrichir ces fonctions et s'interfacer avec d'autres produits sécurité.

Microsoft propose plusieurs niveaux de services, qui intègrent toutes ou parties des fonctions sécurité. Ces niveaux sont détaillés dans le descriptif des services. L'outil **Secure Score**, intégré à la solution, permet d'évaluer le niveau de sécurité de son organisation au sein d'Office 365.

	Par défaut dans toutes les souscriptions Office 365	*Fonctions soumises à des licences additionnelles ou proposées par des tiers*
Gouvernance	• Message Center • Security Center • Compliance Center • Rétention des données	• Système de sauvegarde de données • Système de rétention avancée des données
Hygiène et bonnes pratiques	• Secure Score • Exchange Online Protection	• Système d'analyse comportementale

	○ Antivirus ○ Antispam ○ Anti-spoofing • Configuration par défaut de services	• Système de protection des appareils (Anti-virus, EDR …) • Système avancé d'analyse de la menace (ATP) : Antiphishing, etc.
Gestion des identités et des accès	• Gestion des identités et des droits dans Azure AD pour Office 365 • MFA pour Office 365 Apps • Security Defaults (incluant MFA) • MDM for Office 365	• Système de contrôle d'accès conditionnel • Système de protection des authentifiants • Système de gestion des appareils (Intune) • Système de gestion des applications • Système de gestion des privilèges • Système de revue des accès
Protection de l'information	• Rétention des données • Intégration du chiffrement et de la signature dans la messagerie	• Système de classification de l'information • Chiffrement des fichiers • Système de gestion des droits numériques (DRM) • Système de protection des accès au cloud (CASB) • Data Loss Prevention (DLP) pour la prévention contre la fuite de données sensibles • Système de localisation des données
Détection des événements sécurité	• Azure Sentinel • Alertes de sécurité • Journalisation des événements	• Système d'alerte avancé basé sur l'analyse comportementale et l'intelligence artificielle • Système de surveillance des accès au cloud (CASB) • Système de gestion des événements de sécurité (SIEM)
Traitement des risques réglementaires	• Compliance Manager • Recherche de contenus pour les administrateurs	• Système de gestion des clés de chiffrement • eDiscovery : pour aider la recherche électronique de documents

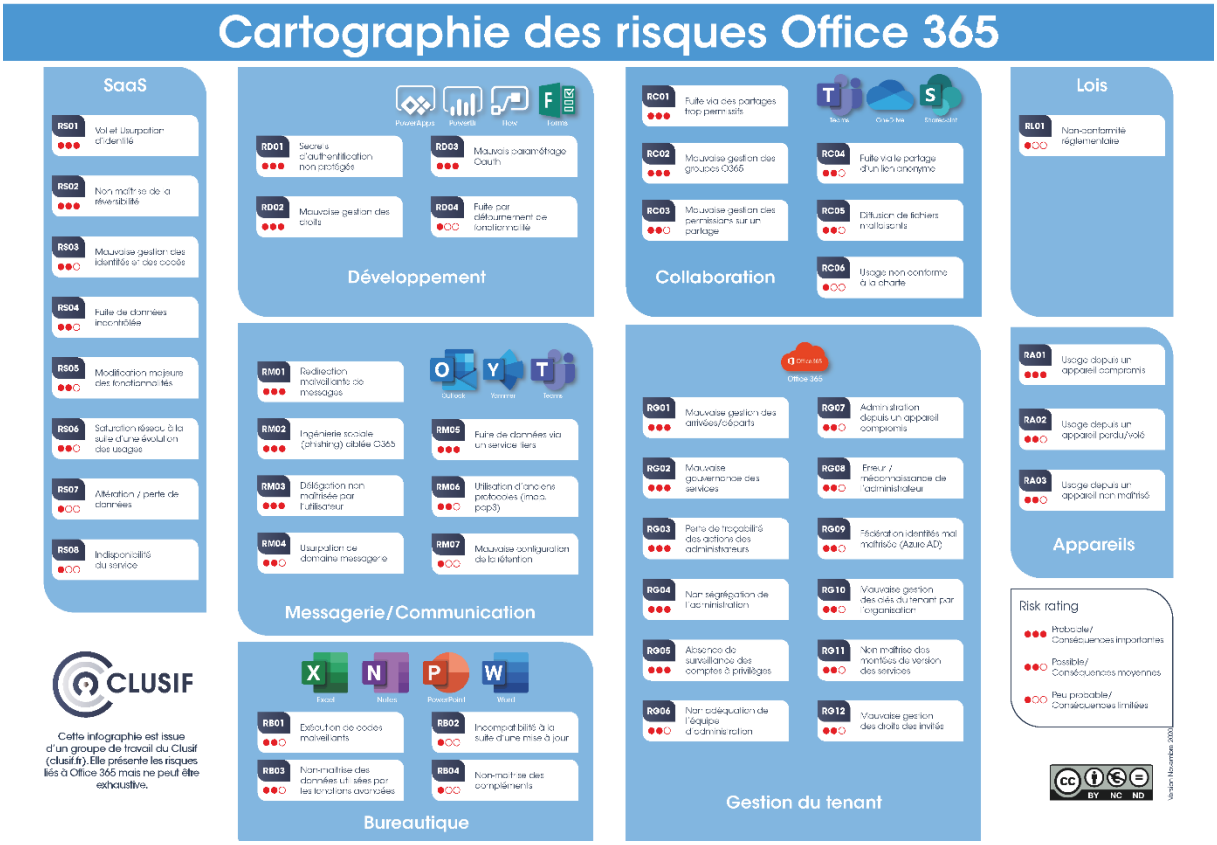
Fonctions Sécurité Office 365

Liens utiles :

Lien vers la chaîne de vidéos mensuelles sur les nouveautés Microsoft 365	https://cutt.ly/AhYcG9d
Lien sur les formations gratuites Microsoft Learn	https://docs.microsoft.com/fr-fr/learn/
Lien sur le CIS Benchmark	https://www.cisecurity.org/benchmark/microsoft_office/
Lien vers la description des services Microsoft	https://www.microsoft.com/fr-fr/licensing/product-licensing/products
Lien vers la synthèse des outils de veille Microsoft 365	https://aka.ms/O365UpdateScout
Lien vers le blog Sécurité et Compliance de Microsoft	https://techcommunity.microsoft.com/t5/microsoft-security-and/bg-p/MicrosoftSecurityandCompliance
Lien vers la documentation Microsoft 365	https://docs.microsoft.com/fr-fr/microsoft-365/

III. Comprendre les risques

Les risques identifiés par le groupe de travail du Clusif sont présentés dans la cartographie reproduite ci-dessous. Un sous-chapitre décrit chacune des familles de risques symbolisés par les blocs dans l'illustration.

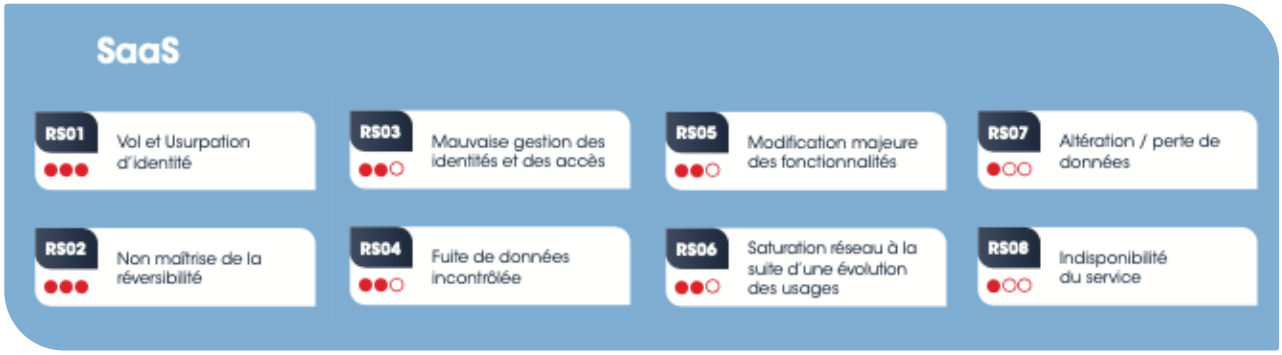


Cartographie des risques

Chaque risque est présenté dans les sous-chapitres suivants avec :

- une description du risque synthétique ;
- un exemple qui illustre le risque ;
- les principales mesures, détaillées dans le chapitre suivant.

III.1. Risques SaaS



RS : Risque SaaS

III.1.1. RS01 Vol et usurpation d'identité

L'usurpation d'identité est le fait de prendre délibérément l'identité d'une autre personne, généralement dans le but de réaliser des actions frauduleuses.

Une identité volée peut être utilisée pour interagir avec d'autres ressources Office 365 ou pour accéder à des ressources internes.

Exemple

Un message usurpant une identité de confiance est utilisé pour inciter un utilisateur à cliquer sur un lien l'amenant à révéler ses identifiants (principe d'hameçonnage, ou phishing).

L'impact est potentiellement fort dans le cas des identités avec privilèges d'accès élevés à des données sensibles (stratégiques ou à caractère personnel) ou des comptes à pouvoir (administrateurs). La probabilité d'occurrence est forte, le phishing étant le type d'attaque le plus courant et le plus efficace pour s'approprier l'identifiant et le mot de passe de la personne.

Plus d'informations

Le principe d'hameçonnage repose sur l'envoi d'un message ciblé à une personne pour lui soustraire l'identifiant et le mot de passe lui donnant accès au réseau de l'organisation. Un attaquant qui aura subtilisé les informations d'authentification pourra accéder à Office 365 pour le compte de l'utilisateur.

Les services en ligne comme Office 365 sont directement accessibles depuis Internet et sont exposés à des attaques qui effectuent des tentatives de connexion sur de nombreuses identités en utilisant les mots de passe les plus fréquents. Ce type d'attaque est plus difficile à détecter que les attaques en force brute et minimise les risques de blocage de comptes.

Mesures

- CMI–1 Mettre en place une authentification renforcée
- CMD-2 Monitorer les usages

III.1.2. RS02 Non-maîtrise de la réversibilité

La réversibilité est la possibilité, pour un client de récupérer ses données et services d'Office 365 s'il met un terme à son contrat.

Exemple

Une organisation change de stratégie et souhaite revenir sur un modèle d'hébergement interne. Lors de l'étude de migration, elle s'aperçoit que la récupération de l'intégralité de ses données brutes et des extensions développées, comme les applications SharePoint sera très

complexe, voire impossible, et qu'elle ne sera pas en mesure d'assurer un service équivalent à Yammer.

Plus d'informations

Dans l'utilisation d'un service en ligne comme Office 365, le principe est que le client reste propriétaire de ses données et peut à tout moment choisir de les reprendre s'il souhaite se désengager du service en ligne. Selon les termes du contrat de service en ligne (OST), le client a la possibilité d'accéder à ses données sur chaque service en ligne, de les en extraire et de les supprimer pendant toute la durée de l'abonnement. En fin de contrat, les données sont conservées encore 90 jours avec des services à fonctionnalité réduite afin de permettre au client de récupérer ses données.

La récupération des composants développés par les métiers (bots, extension Office, applications SharePoint, etc.) sera en revanche plus complexe à mettre en œuvre.

Termes des contrats de licence	https://www.microsoft.com/fr-fr/licensing/product-licensing/products

Cependant, cette réversibilité pourra être plus ou moins facile selon que le service existe ou non sous une forme « non-cloud ».

Mesures

- **CMG-8 Maîtriser les transferts de données (réversibilité)**

III.1.3. RS03 Mauvaise gestion des identités et des accès

L'accès à Office 365 doit être intégré dans le processus de l'entreprise gérant les utilisateurs du système d'information afin que les administrateurs du locataire (tenant) Office 365 soient en mesure de gérer correctement les accès à la messagerie, aux partages de fichiers et aux autres fonctionnalités d'Office 365.

Une mauvaise gestion des utilisateurs par des processus inadaptés peut avoir des conséquences graves telles que la fuite de données ou encore la non-conformité réglementaire. Cela concerne en particulier les personnes quittant l'organisation, qui doivent être signalées aux administrateurs pour supprimer les accès selon la politique de sécurité de l'organisation.

Exemple

Lorsqu'un projet se termine, les personnes externes à l'organisation gardent leur accès à Office 365 tant que le responsable du projet ne signale pas leur départ au support Office 365. Les documents du projet restent accessibles à ces personnes, ainsi que les données échangées sur les Teams auxquels elles avaient accès.

Mesures

- **CMI–3 Mettre en place une revue des comptes et privilèges**
- **CMD-3 Monitorer les accès aux données**

III.1.4. RS04 Fuite de données incontrôlée

La fuite de données consiste en une divulgation inopportune de données qui met en cause la sécurité de l'information. Elle peut provenir d'un utilisateur malveillant ou d'une erreur d'utilisation.

Pour rappel, en cas de violation (perte de disponibilité, d'intégrité ou de confidentialité de données personnelles, de manière accidentelle ou illicite) de données à caractère personnel, une déclaration à la CNIL ou à l'autorité compétente est à réaliser dans les 72 heures et

informer les personnes concernées (cf https://www.cnil.fr/fr/reglement-europeen-protection-donnees/chapitre4#Article35).

Dans le cas d'Office 365, l'identification des données impactées peut être un enjeu à part entière en raison de la nature non structurée des données (fichiers bureautiques, images, etc.).

Lorsque les éléments de preuve sont suffisants et si le préjudice est quantifiable, il est vivement encouragé de déposer une plainte.

Exemple

Un utilisateur donne accès à des informations sensibles *via* un partage SharePoint malencontreux. L'utilisateur externe accéde à cet espace SharePoint et ainsi à des données confidentielles.

Mesures

- **CMP-2 Protéger les informations sensibles par chiffrement**
- **CMD-2 Monitorer les usages**

III.1.5. RS05 Modification majeure des fonctionnalités

Avec les services cloud tels qu'Office 365, une approche d'innovation en continu est introduite. L'éditeur fait évoluer de façon régulière ses solutions ou fonctionnalités : nouveautés, mises à jour, suppressions. Ces évolutions peuvent avoir des conséquences importantes telles qu'une non-conformité réglementaire ou encore une exposition à de nouveaux risques.

Exemple

Microsoft fait l'acquisition d'une nouvelle société et introduit une nouvelle solution au sein de la suite Office 365. Les données de cette application sont stockées aux États-Unis uniquement, ce qui pourrait entraîner une non-conformité par rapport à la politique interne de l'entreprise.

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**
- **CMG-8 Maîtriser les transferts de données (Réversibilité)**

III.1.6. RS06 Saturation réseau à la suite d'une évolution des usages

Le réseau interne et la sortie Internet de l'organisation peuvent être mal dimensionnés et ne pas pouvoir absorber les augmentations de trafic. Un dimensionnement inadéquat impactera les utilisateurs en dégradant les performances des services utilisés ou en les rendant pratiquement inutilisables en cas de forte saturation.

Exemple

L'organisation décide de modifier ses processus internes en promouvant l'usage de Teams, en modernisant sa communication *via* des vidéos partagées *via* Stream ou en migrant massivement des arborescences de fichiers dans SharePoint Online ou OneDrive. L'explosion de l'usage de ces services entraîne une augmentation du trafic réseau interne et/ou Internet qui impacte fortement les infrastructures réseau et sécurité existantes.

La synchronisation de répertoires, contenant potentiellement des fichiers volumineux ou des archives de messagerie stockés sur OneDrive génère des échanges importants avec les infrastructures Microsoft sollicitant d'autant plus les appareils réseaux et sécurité (firewalls et proxies).

Mesures

- **CMH-9 Surveiller les performances des infrastructures d'accès et augmenter la bande passante si nécessaire**

III.1.7. RS07 Altération/Perte de données

Un utilisateur ayant des droits de modification sur une donnée est en mesure de la supprimer ou de la modifier.

Une erreur ou une action malveillante pourrait ainsi entraîner l'altération ou la perte de données de l'organisation.

Pour rappel, une altération de données peut être soumise aux contraintes CNIL.

Plus d'informations

Selon le service, un système de corbeilles à plusieurs niveaux permettra de conserver les données un certain temps (93 jours pour SharePoint Online, 30 jours pour OneDrive for Business et jusqu'à 30 jours pour Exchange Online), avant suppression définitive.

À noter, Microsoft réalise des copies de l'ensemble des sites SharePoint toutes les 12 heures et les conserve pendant 14 jours. Une copie d'un site ou d'un sous-site peut être restaurée sur demande au support.

L'altération et la perte peuvent également être réalisées par des utilisateurs ayant effectué une erreur de manipulation.

Exemples

Un utilisateur remarque des erreurs lors de la synchronisation d'une bibliothèque de fichiers SharePoint avec son poste de travail. En tentant de résoudre ce problème, il supprime une partie de l'arborescence sur son poste de travail sans arrêter la synchronisation. La suppression des éléments est ainsi répercutée dans les données cloud.

Un utilisateur malveillant accède au locataire (tenant) Office 365 et supprime des données pour nuire à l'organisation ou encore cacher ses traces à la suite d'une attaque. Une variante consiste à altérer les données dans le but de monnayer la récupération des données (ransomware).

Mesures

- **CMG-3 Définir une stratégie de rétention des données**
- **CMD-3 Monitorer les accès aux données**

III.1.8. RS08 Indisponibilité du service

Bien qu'ils répondent à des critères précis et à des certifications, les centres de données et services de Microsoft ne sont pas à l'abri d'une défaillance. Elle peut être technique, organisationnelle ou humaine.

Exemple

Un incident technique impacte la solution de gestion des identités Azure Active Directory. Les employés ne sont plus en mesure de s'authentifier pour accéder aux solutions Office 365.

Plus d'informations

L'engagement de disponibilité des services est détaillé dans un document contractuel (Service Level Agreements for Microsoft Online Services, SLA) où la disponibilité minimale au-delà de laquelle le client peut prétendre à une indemnité est précisée par service. Pour la plus grande partie des services Office 365, la disponibilité minimale est de 99,9 % (Exchange Online, SharePoint Online, OneDrive Entreprise, etc.).

Cependant, le SLA réel mesuré est supérieur à cette valeur puisque pour les 2 premiers trimestres de 2019, il était de 99,97 % ce qui correspond à un temps d'indisponibilité de 12 minutes 57 secondes sur un mois.

Certaines applications et certains services offrent la possibilité de continuer à travailler hors-ligne : par exemple, les versions desktop de la suite Office incluses dans la licence de base sous la forme Microsoft 365 Apps (Word, Excel, Outlook, OneNote, etc.) permettent de continuer à travailler en mode déconnecté. Le client OneDrive offre l'accès aux versions des fichiers en local et synchronise automatiquement les mises à jour lorsque la connexion au service redevient disponible. De même, certaines applications Web comme Outlook Web Access possèdent aussi la capacité à travailler en mode offline.

En revanche, des services de communication comme Exchange Online (messagerie), Teams (chat, téléphone IP…) ne pourront pas être utilisés tant que l'accès au service ne sera pas rétabli.

Ce qui peut être pris comme une indisponibilité du service Office 365 peut être lié à d'autres éléments comme des problèmes réseau ou un service interne de fédération d'identités.

Licensing Terms and Documentation (version française)	https://www.microsoftvolumelicensing.com
État de santé des services et continuité	https://docs.microsoft.com/fr-fr/office365/servicedescriptions/office-365-platform-service-description/service-health-and-continuity

Mesures

- **CMH-8 Faciliter le travail en mode déconnecté**
- **CMH-11 Déterminer l'indisponibilité effective du service Office 365**

III.2. Risques Appareil

RA : Risque Appareil

III.2.1. RA01 Usage depuis un appareil compromis

Un utilisateur accédant aux services Office 365 depuis un appareil compromis donne la possibilité à un attaquant de récupérer ou d'altérer les documents traités ou téléchargés sur l'appareil ou les informations saisies sur les interfaces Web d'Office 365.

Plus d'informations

Ce risque n'est pas lié directement à Office 365, mais plus largement à la gestion de la sécurité de l'appareil de l'utilisateur et au choix d'autoriser ou non l'accès depuis un appareil non géré.

Il est recommandé que tous les appareils maîtrisés soient équipés d'une solution de protection, de détection et de réponse. Ces solutions peuvent s'interfacer avec les outils de MDM pour remonter des informations quant à l'état de santé et de conformité de l'appareil.

Cet état de santé et de conformité du terminal pourra être utilisé lors de la vérification de la politique d'accès conditionnel.

Exemples

- L'utilisateur se connecte à Office 365 depuis son appareil sur lequel est installé à son insu un malware. Ce dernier envoie à un attaquant externe une copie de tous les documents que l'utilisateur synchronise sur OneDrive.
- Un appareil est infecté par un rançongiciel. Les documents chiffrés à leur tour sont alors synchronisés vers OneDrive ou vers SharePoint.

Mesures

- **CMH-1 S'équiper contre les codes malveillants**
- **CMP-2 Protéger les informations sensibles par chiffrement**
- **CMP-5 Gérer les applications avec un outil de gestion des applications mobiles**
- **CMP-6 Mettre en place le contrôle d'accès conditionnel**
- **CMD-3 Monitorer les accès aux données**

III.2.2. RA02 Usage depuis un appareil perdu/volé

Lorsqu'un utilisateur synchronise sa messagerie, son OneDrive ou des répertoires SharePoint Online, il copie sur son appareil des données de l'entreprise. En cas de vol ou de perte de son appareil, la personne qui récupère le matériel pourrait avoir accès à ses données.

Exemple

Pour des raisons pratiques, Pierre, directeur d'une entreprise, synchronise sa messagerie et tout son OneDrive sur son appareil personnel non chiffré et sans mot de passe. À la suite d'un vol à son domicile, le voleur accède à toutes les données sensibles de l'organisation gérée par Pierre.

Plus d'informations

La première mesure consiste à sensibiliser les utilisateurs, d'autant plus ceux ayant accès à des informations sensibles, de ne pas utiliser un appareil dont la sécurité n'est pas conforme aux politiques de sécurité de l'organisation.

Il est également possible d'utiliser des mesures techniques pour bloquer le transfert de données de messagerie ou de OneDrive sur un appareil non conforme. Enfin, le chiffrement des données sensibles et la restriction des droits associés les rendront inaccessibles en cas de vol puisqu'une authentification sera nécessaire pour y accéder.

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMI–1 Mettre en place une authentification renforcée**
- **CMI–5 Maîtriser les appareils autorisés à accéder à Office 365**
- **CMP-2 Protéger les informations sensibles par chiffrement**
- **CMP-6 Mettre en place le contrôle d'accès conditionnel**
- **CMP-7 Interdire la synchronisation des données depuis les appareils non gérés**

III.2.3. RA03 Usage depuis un appareil non maîtrisé

Par défaut, un utilisateur peut se connecter à un service Office 365 et synchroniser des données depuis n'importe quel appareil. Bien que les avantages en termes de mobilité soient évidents, la question de l'encadrement des usages mobiles se pose.

En effet, la connexion à Office 365 sur un appareil non maîtrisé par l'entreprise pourrait exposer les données dans le cas où l'utilisateur synchronise des fichiers en local ou ne se déconnecte pas dans son navigateur.

D'une manière plus générale, il s'agit de savoir si on autorise ou non l'accès à Office 365 depuis des appareils non gérés par l'organisation.

Ce risque porte essentiellement sur la synchronisation en local de la messagerie et de répertoires OneDrive. Il concerne tous les types d'appareils (mobile, poste de travail) qui n'apportent pas tous le même niveau de protection des données qu'ils stockent. Cela pose aussi la question de la séparation entre les données professionnelles et personnelles lorsque les accès à Office 365 sont réalisés depuis un appareil personnel.

Pour aller plus loin, une mauvaise gestion des jetons de session Office 365, qui par défaut sont persistants, pourrait permettre à une personne non autorisée d'accéder au profil et aux données du portail Web Office 365 d'un utilisateur précédemment connecté sur un appareil.

Enfin, de manière plus stricte, on peut interdire l'accès à Office 365 depuis un appareil non géré par l'organisation ou restreindre l'accès en lecture seule.

Exemples

L'utilisateur s'est connecté sur son compte Office 365 depuis un appareil personnel et a simplement fermé par la suite son navigateur Web. Une personne tierce accédant à cet appareil (de façon légitime ou non) peut accéder au portail et aux données, sans nouvelle demande d'authentification.

Le cas d'une connexion à un appareil d'hôtel en libre-service ou depuis un cybercafé est similaire.

Plus d'informations

Microsoft propose en option une fonctionnalité d'accès conditionnel. Cette fonctionnalité permet de définir une politique d'accès à Office 365 en prenant en compte des critères sur l'appareil utilisé et la confiance donnée à l'utilisateur.

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMI–5 Maîtriser les appareils autorisés à accéder à Office 365**
- **CMP-5 Gérer les applications avec un outil de gestion des applications mobiles**
- **CMP-6 Mettre en place le contrôle d'accès conditionnel**
- **CMG-6 Mettre en place une gestion stricte des licences**
- **CMD-3 Monitorer les accès aux données**

III.3. Collaboration

RC : Risque Collaboration

III.3.1. RC01 Fuite via des partages trop permissifs

Un utilisateur ne maîtrisant pas les mécanismes d'allocation de droits d'un outil collaboratif (SharePoint Online, OneDrive for Business, Power BI, etc.) pourrait facilement et involontairement mettre à disposition des informations à un tiers.

Plus d'informations

L'expérience utilisateur pour le partage de contenu d'un service Office 365 (SharePoint Online, OneDrive for Business, Microsoft 365 Apps, etc.) est identique. Lorsqu'un utilisateur partage un document ou un fichier, un lien de partage est automatiquement créé avec des permissions associées.

Il existe quatre types de permissions :

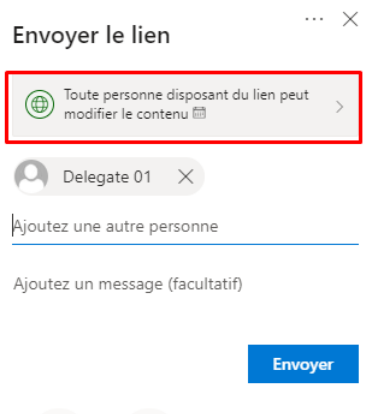
- **toute personne disposant du lien ;**
- **toute l'organisation ;**
- **personnes ayant déjà un accès ;**
- **personne spécifique.**

Toute personne remplissant la condition et disposant du lien pourra accéder au document partagé.

Exemple

Prenons le cas d'une organisation qui a autorisé la création de lien anonyme et a fixé le type de lien sélectionné par défaut à « Toute personne disposant du lien ».

Dès lors, pour tout partage, même si un utilisateur est nommé dans le partage, le lien qui sera créé par Office 365 permet à toute personne possédant ce lien d'accéder au fichier. Il est recommandé d'associer une expiration du lien d'accès à quelques jours.



Partage de lien

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMH-2 Durcissement des configurations des services de collaboration**
- **CMD-3 Monitorer les accès aux données**

III.3.2. RC02 Mauvaise gestion des groupes Office 365

Une mauvaise mise à jour des personnes appartenant à un groupe Office 365 peut permettre à une personne d'accéder à des ressources disponibles dans un espace collaboratif (SharePoint Online, Teams, Power BI, etc.), alors qu'elle n'est pas censée en avoir l'autorisation.

Plus d'informations

À la différence de la gestion des permissions SharePoint Online, les groupes Microsoft 365 proposent trois niveaux de droits :

- **propriétaire :** les propriétaires de groupe peuvent ajouter ou supprimer des membres et avoir des autorisations uniques, telles que la possibilité de supprimer des éléments, ou de modifier des paramètres (ex. : le nom du groupe, la description ou la visibilité) ;
- **membre :** les membres peuvent accéder à tous les éléments du groupe, mais ils ne peuvent pas modifier les paramètres du groupe. Par défaut, les membres peuvent inviter des invités à rejoindre votre groupe ;
- **invités :** les invités de groupe sont membres de l'extérieur de votre organisation.

À noter, un « propriétaire » est équivalent à un « administrateur » de site pour le site SharePoint Online sous-jacent.

Exemple

Pierre a quitté le service comptabilité pour rejoindre le département des achats, mais comme ce changement de fonction n'a pas été pris en compte dans le groupe « Office 365-comptabilité », il peut toujours avoir accès aux fichiers de son ancien service.

De plus, il était propriétaire du groupe en question. Il peut également ajouter de nouvelles personnes.

Mesures

- **CMH-2 Durcissement des configurations des services de collaboration**
- **CMI-2 Mettre en place une gestion des arrivées/départs**
- **CMD-3 Monitorer les accès aux données**

III.3.3. RC03 Mauvaise gestion des permissions sur un partage

Un utilisateur ne maîtrisant pas les mécanismes de gestion des permissions d'accès d'un outil collaboratif (SharePoint Online, OneDrive for Business, etc.) donne plus de droits que nécessaire, aux utilisateurs pouvant avoir accès à ces ressources partagées.

Plus d'informations

En plus du périmètre du lien de partage évoqué dans le paragraphe RC01, il existe d'autres paramètres permettant de limiter les actions d'un utilisateur sur un document ou un dossier.

Les utilisateurs doivent être informés que la gestion des droits porte sur :

- le périmètre du partage (« Personnes autorisées à utiliser le lien ») ;
- la capacité de lecture/écriture ;
- la capacité à restreindre le téléchargement ;
- la durée du lien de partage ;
- la protection par un mot de passe.

Un autre cas d'usage porte sur la durée des permissions données par un utilisateur sur ses fichiers. Les permissions sont souvent ajoutées, mais rarement, voire jamais, retirées. Dans ce cas, un utilisateur ayant le droit d'accéder à un répertoire sera en mesure de consulter les nouveaux fichiers, qui ne seraient pas destinés à tous ceux qui ont des permissions.

Partager des fichiers ou dossiers SharePoint	https://support.office.com/fr-fr/article/partager-des-fichiers-ou-dossiers-sharepoint-1fe37332-0f9a-4719-970e-d2578da4941c

Exemple

Alors qu'un document a uniquement besoin d'être consulté, l'utilisateur donne les droits d'écriture sur ce fichier. Une personne ayant accès à ce document pourra alors, par mégarde, modifier ou même supprimer ce document, alors que si cet individu n'avait eu que les droits de lecture il n'aurait pas pu commettre cette erreur.

Mesures

- **CMH-2 Durcissement des configurations des services de collaboration**
- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMD-3 Monitorer les accès aux données**

III.3.4. RC04 Fuite *via* le partage d'un lien anonyme

Un utilisateur partage un fichier stocké dans un outil collaboratif (SharePoint Online, OneDrive for Business, Power BI, etc.) grâce à un lien anonyme.

Ce lien vient à être connu d'une tierce partie qui prend connaissance du contenu du fichier alors qu'elle n'aurait pas dû y avoir accès, et ce, sans avoir à s'authentifier.

Pour aller plus loin

Par défaut, lorsqu'un utilisateur fait un partage, la configuration des locataires (tenants) Office 365 crée un lien de type anonyme, qui peut être changé *via* une fenêtre déroulante lors du partage.

Si la configuration par défaut n'est pas modifiée par les administrateurs, il est donc très facile de se tromper et de partager anonymement un document de manière tout à fait involontaire.

Exemple

Le service des ressources humaines souhaite partager la politique d'augmentation de l'année en cours à l'ensemble des responsables RH de l'organisation. Comme il y a plus d'une centaine de destinataires, la personne en charge de la diffusion préfère passer par un lien anonyme plutôt que de gérer unitairement les accès. Malheureusement, des personnes non habilitées reçoivent ce document.

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMH-2 Durcissement des configurations des services de collaboration**

- **CMD-2 Monitorer les usages**
- **CMD-3 Monitorer les accès aux données**

III.3.5. RC05 Diffusion de fichiers malveillants

Un utilisateur met à disposition ou contamine un fichier dans un espace collaboratif (SharePoint Online, OneDrive for Business, etc.) avec un malware (ex. : macro Excel malveillante). Toutes les personnes qui vont consulter ce fichier seront ensuite contaminées. Ce risque comprend les actions volontaires d'un utilisateur malveillant et les actions involontaires d'un utilisateur négligent.

Plus d'informations

SharePoint embarque nativement un antivirus. Lorsqu'un fichier est détecté comme malveillant, il ne pourra pas être téléchargé ou synchronisé.

À noter que la précédente limite de 25 Mo des fichiers a été levée.

Exemple

Le fils du chef de département consulte sa messagerie personnelle sur l'ordinateur familial et par mégarde se retrouve infecté par un virus macro en consultant un fichier Excel proposant un test de personnalité. Le chef de département utilisant ce même ordinateur pour mettre à jour un fichier, sur un site SharePoint de l'organisation, le contamine à son tour.

Mesures

- **CMH-2 Durcissement des configurations des services de collaboration**
- **CMP-6 Mettre en place le contrôle d'accès conditionnel**

III.3.6. RC06 Usage non conforme à la charte

Un utilisateur utilise les ressources collaboratives de l'organisation pour un usage non conforme à la charte des bons usages des moyens informatiques de l'organisation.

Exemple

Un utilisateur télécharge sur Internet le dernier épisode d'une série en vogue et le met à disposition de ses collègues *via* un partage SharePoint Online ou Stream. Il peut ainsi exposer son organisation à d'éventuelles poursuites des ayants droit de cette série.

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMH-2 Durcissement des configurations des services de collaboration**

III.4. Messagerie/Communication

RM : Risque Messagerie

III.4.1. RM01 Redirection malveillante de messages

Par défaut, une personne peut configurer une règle de transfert automatique de tout ou partie du flux de messagerie d'un utilisateur, vers une adresse tierce.

Bien que ces fonctionnalités soient utiles pour, par exemple, transférer le contenu des messages reçus par un utilisateur ayant quitté l'organisation vers son remplaçant sans donner un accès complet à la boîte aux lettres de celui-ci, elles peuvent également offrir des possibilités pour un utilisateur malveillant.

Plus d'informations

Il existe plusieurs façons de créer des règles de redirection automatique :

- un utilisateur peut créer une règle Inbox dans son client Outlook ou un script ;
- un utilisateur peut créer une série d'actions automatisées, *via* PowerAutomate ;
- un administrateur peut créer des règles de transfert de type SMTP_Forward, Journal Rules, Transport Rules.

Exemple

À la suite de la compromission de la messagerie du directeur d'une entité, une règle de transfert automatique est mise en place afin de conserver un accès persistant aux messages du compte, même dans le cas d'un changement de mot de passe.

Que ce soit coté serveur ou coté client, une règle de classement automatique des emails peut également être mise en place. Elle permet au pirate de masquer au propriétaire certains emails contenant par exemple des identifiants de paiement et de ultérieurement lui envoyer des emails crédibles contenant des identifiants de paiement modifiés.

Mesures

- **CMH-3 Durcissement des configurations des services de messagerie**
- **CMD-2 Monitorer les usages**

III.4.2. RM02 Ingénierie sociale (phishing) ciblée Office 365

Les millions d'utilisateurs professionnels de la suite Office 365 font l'objet de tentatives de phishing toujours plus nombreuses et sophistiquées.

En plus des techniques de phishing et de spear phishing habituelles, les utilisateurs d'Office 365 peuvent être victimes d'un certain nombre d'attaques.

Plus d'informations

Par défaut, les informations de l'annuaire sont accessibles en lecture à l'ensemble des utilisateurs de l'organisation. Un utilisateur interne peut accéder à ces informations *via* le Portail Azure, PowerShell ou les API Graph. Un utilisateur invité peut également avoir accès à tout ou partie de l'annuaire en lecture.

Plusieurs attaques ont été identifiées ces derniers temps, ayant pour objectif de cartographier l'organisation avant de lancer des campagnes de phishing ciblées.

Exemple

Des messages malveillants contiennent des redirections vers de faux portails d'authentification similaires à Office 365 ou à une page d'authentification légitime derrière laquelle se trouve une application malveillante requérant des permissions sur les données de l'utilisateur (cf. RD03 Mauvais paramétrage OAuth).

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMH-3 Durcissement des configurations des services de messagerie**
- **CMD-2 Monitorer les usages**

III.4.3. RM03 Délégation non maîtrisée par l'utilisateur

Un utilisateur ne maîtrisant pas les mécanismes de gestion des permissions d'accès Outlook donne plus de droits que nécessaire sur ses messages ou son calendrier.

Plus d'informations

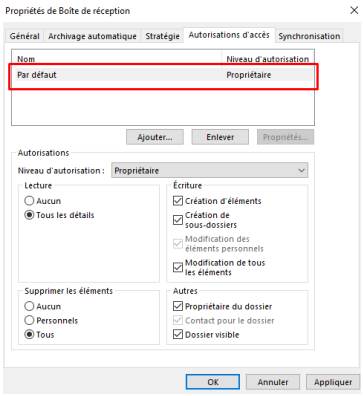
Exchange Online permet de donner des permissions d'accès à tout ou partie d'un compte de messagerie à d'autres utilisateurs.

L'affectation de ces permissions est silencieuse, aucune notification n'est émise par Exchange Online.

Il est important de garder en tête que la gestion des permissions est complexe à maîtriser dans le temps. Il n'est pas rare de trouver des permissions qui n'ont plus raison d'être. De même, il est fréquent de trouver des « doubles permissions » (une permission de type « accès complet » et une permission de type « accès partiel »).

Exemple

Un utilisateur souhaite assigner une nouvelle délégation à un collègue. Il sélectionne par inadvertance le compte « Default » et donne involontairement accès à l'ensemble de l'organisation à son dossier.



Exemple de délégation

Mesures

- **CMH-3 Durcissement des configurations des services de messagerie**
- **CMD-2 Monitorer les usages**

III.4.4. RM04 Usurpation de domaine de messagerie

Aujourd'hui, les attaquants s'approprient sans aucun scrupule des noms de domaine qui ne leur appartiennent pas pour véhiculer des spams. De ce fait, non seulement les filtres antispam sont de plus en plus sollicités, mais cela conduit également parfois à exclure les noms de domaine en question qui font du tort et nuisent au bon déroulement des communications.

Exemple

Une entreprise utilise un service de mass-mailing. Pour ne pas être bloquée par les systèmes antispam, elle déclare une exception sur les adresses IP ou domaines messageries utilisés par son fournisseur. Ce fournisseur proposant des tests gratuits accessibles par tous, un utilisateur malveillant utilise cette opportunité de test pour une campagne de phishing qui ne sera pas bloquée du fait de l'exception configurée.

Mesures

- **CMH-3 Durcissement des configurations des services de messagerie**

III.4.5. RM05 Fuite de données *via* un service tiers

L'utilisation d'applications ou de services tiers lors de la manipulation des données stockées sur Office 365 peut entraîner une surexposition qui pourrait aboutir à une fuite intentionnelle ou non.

Exemple

L'utilisation d'un client de messagerie différent d'Outlook sur un terminal mobile et non supporté par les politiques de Mobile Application Management, pourrait permettre à l'utilisateur de contourner les politiques de sécurité.

Mesures

- **CMP-3 Limiter les droits d'accès aux documents partagés en externe**
- **CMP-2 Protéger les informations sensibles par chiffrement**
- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**

III.4.6. RM06 Utilisation d'anciens protocoles (IMAP, POP3)

L'utilisation de l'authentification basique (identifiant et mot de passe) pour les protocoles de messagerie EWS (Exchange Web Services), EAS (Exchange ActiveSync), IMAP4, POP3 et RPS (Remote PowerShell) sera dépréciée au 2e semestre 2021 pour des raisons de sécurité, et remplacée par l'authentification « moderne » OAuth permettant de supporter entre autres l'authentification multifacteur.

Exemple

Certaines applications anciennes utilisent le protocole IMAP pour synchroniser les messages, qui ne supporte pas les mécanismes de double authentication (MFA). Un login/password est compromis suite à une campagne de phishing réussie. L'attaquant utilise le protocole IMAP pour se connecter à la messagerie.

https://developer.microsoft.com/en-us/office/blogs/end-of-support-for-basic-authentication-access-to-exchange-online-apis-for-office-365-customers/

Mesures

- **CMH-3 Durcissement des configurations des services de messagerie**
- **CMP-6 Mettre en place le contrôle d'accès conditionnel**
- **CMD-2 Monitorer les usages**

III.4.7. RM07 Mauvaise configuration de la rétention (messagerie)

Une mauvaise configuration des politiques de rétention de l'organisation pourrait entraîner une non-conformité réglementaire ou une perte de données.

En effet, les éléments de messagerie comme les fichiers ne sont pas supprimés, sauf après une action manuelle ou application d'une politique de rétention.

Office 365 n'offre pas de fonctionnalités de sauvegarde à proprement parler, il est nécessaire d'analyser les principes de rétention applicables à l'organisation et la nécessité d'acquérir un outil de sauvegarde tiers.

Plus d'informations

La capacité d'une boîte aux lettres Exchange Online dépend du type de boîte aux lettres et de la licence Office 365 de l'utilisateur concerné (entre 2 Go et 100 Go).

Les politiques de rétention peuvent être définies de plusieurs façons dans Office 365, en fonction des besoins :

- les étiquettes de rétention permettent de configurer les modalités de conservation et de suppression applicables à des éléments de messagerie ou des fichiers (définies dans les centres de sécurité et de conformité) ;
- les stratégies de Litigation Hold et de In Place Hold permettent de définir les règles de conservation applicables aux boîtes aux lettres afin de conserver une trace en cas de litige (définies dans le centre d'administration Exchange).

À noter, dans le cadre d'un cas eDiscovery, une partie des éléments de messagerie peut également être gelée le temps de l'investigation.

Exemple

Dans le cadre de son plan de mise en conformité avec le RGPD, une organisation décide de supprimer automatiquement tous les messages ayant plus de 3 ans. Un département de l'organisation utilisant la messagerie pour l'ensemble de ses échanges pourrait perdre une partie de ses données. De même, une erreur d'administration sur les politiques de rétention pourrait aboutir à la suppression de données de l'entreprise.

Dans le cadre d'une enquête, une organisation est tenue de fournir une copie de tous les messages d'un cadre dirigeant de l'année passée. L'organisation n'a pas implémenté de politique de rétention permettant de répondre à ce besoin.

Mesures

- **CMH-3 Durcissement des configurations des services de messagerie**

III.5. Développement

RD : Risque Développement

III.5.1. RD01 Secrets d'authentification non protégés

Une mauvaise gestion des secrets comme la présence de mots de passe ou de clés d'API dans le code de script ou code source développé en interne peut permettre à un attaquant d'accéder à des ressources de la souscription Office 365.

Plus d'informations

Office 365 est propice aux intégrations avec des applications du marché ou développées en interne. Ces applications peuvent être destinées à des fins d'administration du locataire (tenant) ou pour créer de nouveaux services pour les utilisateurs.

La plupart des applications utilisent des secrets d'applications. Ces mots de passe ou certificats sont utilisés pour accéder aux API Microsoft ou se connecter à des API tierces. La présence de ce secret dans le code source de l'application ou dans les paramètres (comme ceux d'une fonction Azure) entraîne une surexposition de ces crédentiels.

Exemple

Une développeuse Web stocke le code source d'une application interagissant avec un service Office 365 sur son appareil. À la suite d'une compromission de l'appareil, les attaquants récupèrent le code source de l'application et donc un identifiant permettant de se connecter à Office 365.

Mesures

- **CMG-5 Former les administrateurs et les développeurs**
- **CMH-4 Durcissement des configurations des développements**

III.5.2. RD02 Mauvaise gestion des droits

Un compte de service ou une application avec des droits trop élevés dans Office 365 ou dans Azure AD augmente la surface de compromission et l'impact en cas d'attaque.

Plus d'informations

Les rôles Azure AD ou RBAC des différents services Office 365 peuvent être attribués à des comptes de service, des services principaux ou à des groupes de sécurité.

Exemple

Afin de simplifier la gestion des utilisateurs (création, suppression, modification du mot de passe, etc.), un administrateur Office 365 crée un compte de service et lui donne des droits de *Global Administrator* par facilité, sans respecter le principe du moindre privilège. En cas de compromission, ce compte de service pourrait donner accès à l'ensemble des données de la plateforme.

Mesures

- **CMG-5 Former les administrateurs et les développeurs**

- **CMD-1 Monitorer les modifications de configuration**
- **CMD-3 Monitorer les accès aux données**

III.5.3. RD03 Mauvais paramétrage OAuth

Une application tierce malveillante ayant reçu une délégation de permissions de la part d'un utilisateur ou d'un administrateur peut exfiltrer ou modifier de la donnée existante.

Plus d'informations

Office 365 permet l'intégration avec des applications en exploitant les fonctions d'API Management et Microsoft Graph. Les permissions accordées à l'application tierce sont gérées par consentement explicite. En fonction de l'autorisation attribuée, l'application obtient un niveau d'accès lui permettant de réaliser telle ou telle action (ex. : droit de lecture sur les messages de tous les utilisateurs ou droit d'écriture sur le calendrier d'un utilisateur donné).

Deux types de consentement sont disponibles :

- **permissions déléguées** (ou consentement utilisateur) : un utilisateur attribue certaines permissions à un service tiers pour effectuer des actions dans son contexte utilisateur. Certaines permissions peuvent nécessiter l'intervention d'un administrateur ;
- **permissions d'application** (ou consentement administrateur) : un administrateur attribue certaines permissions à un service tiers pour effectuer des actions sur l'ensemble de la plateforme Microsoft 365. Il s'agit principalement d'applications s'exécutant sans qu'un utilisateur soit connecté.

https://docs.microsoft.com/en-us/azure/active-directory/develop/delegated-and-app-perms

Il est important de noter que les possibilités de journalisation des actions d'une application ayant des permissions sont assez limitées.

Exemple

Une application est approuvée par une organisation. Malheureusement, cette application contient une vulnérabilité et une mauvaise permission déléguée a été donnée par l'administrateur.

Un utilisateur valide une application envoyée par un attaquant sans regarder les droits fournis et autorise alors une application malveillante à accéder de façon permanente à ses données.

Mesures

- **CMG-5 Former les administrateurs et les développeurs**
- **CMI–6 Mettre en place un processus de gestion des services tiers**
- **CMD-1 Monitorer les modifications de configuration**
- **CMD-3 Monitorer les accès aux données**

III.5.4. RD04 Fuite par détournement de fonctionnalité

Un utilisateur pourrait intentionnellement s'appuyer sur des capacités et des outils de la plateforme de telle sorte qu'il arrive à exporter de manière massive les données de l'organisation auxquelles il a accès. Il s'agit ici de mettre en avant le risque d'automatiser l'export des données de la part d'un utilisateur qui a légitimement le droit de lire ses fichiers ou ses messages. On ne parle pas ici de mauvaises permissions, mais simplement l'utilisation d'outils automatisant l'export des données en masse dont l'utilisateur a accès dans le cadre de son travail.

Exemple

Un utilisateur en cours de préavis de départ cherche à exfiltrer le maximum de données avant son départ. Il s'appuie sur un tutoriel lui indiquant comment utiliser facilement et sans programmation des fonctionnalités Office 365 pour exporter les données auxquelles il a accès.

Il pourrait par exemple créer :

- Une application PowerApps ou implémenter un workflow PowerAutomate pour transférer sur son espace de stockage personnel tout nouveau document ou nouvelle pièce jointe ;
- Une application Azure avec des permissions de Graph API pour extraire de l'information des sites SharePoint auxquels il aurait accès.

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**
- **CMP-2 Protéger les informations sensibles par chiffrement**
- **CMD-2 Monitorer les usages**

III.6. Bureautique

RB : Risque Bureautique

III.6.1. RB01 Exécution de codes malveillants

Un utilisateur peut exécuter, volontairement ou non, du code malveillant au sein de l'un des produits Microsoft 365 Apps, que ce soit par le biais d'une application locale ou Web.

L'interconnexion de produits Office 365 représente un risque supplémentaire car c'est un facteur facilitant la propagation du code malveillant et augmentant le nombre de données potentiellement accessibles.

https://docs.microsoft.com/en-us/office365/enterprise/office-365-malware-and-ransomware-protection
https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection

Plus d'informations

Par défaut une protection anti-malware est activée dans Exchange Online et SharePoint Online pour se protéger contre les fichiers contenant du code malveillant. Une bonne pratique est de bloquer l'exécution des macros par défaut. Cela peut cependant impacter les utilisateurs qui développent des macros dans leurs documents.

Exemple

Un utilisateur reçoit un message avec un fichier Word attaché. En l'ouvrant, il déclenche du code malveillant qui permet à une personne non autorisée d'accéder à ses documents et de déposer une copie du fichier infecté sur un dossier OneDrive partagé.

Le code malveillant est alors potentiellement accessible par toute l'organisation.

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**
- **CMH-1 S'équiper contre les codes malveillants**

III.6.2. RB02 Incompatibilité à la suite d'une mise à jour

Les produits Office 365 étant hébergés dans le cloud, l'organisation n'a pas la maîtrise du rythme des mises à jour ni des ajouts ou des suppressions de fonctionnalités.

Un script, une fonctionnalité ou même un produit complet peuvent cesser de fonctionner à court ou moyen terme.

https://docs.microsoft.com/fr-fr/deployoffice/change-management-for-office-365-clients

Exemple

Un script Power Automate a été développé par Alexia, utilisatrice avancée, il se base sur une fonctionnalité de récupération de posts Facebook au sein d'Office 365.

Cette fonctionnalité est mise à jour par Microsoft et le mode d'authentification change. Du coup, le script ne fonctionne plus et il faut le déboguer alors qu'il n'a pas été touché depuis plusieurs mois.

Plus d'informations

Les nouveautés et améliorations de Microsoft 365 sont régulièrement actualisées pour décrire bon nombre des nouvelles fonctionnalités d'Office.

https://www.microsoft.com/en-us/microsoft-365/roadmap

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**
- **RB03 Non-maîtrise des données utilisées par les fonctions avancées**

Microsoft 365 Apps monitore d'une certaine façon les usages des utilisateurs. En effet les applications envoient des données anonymisées vers le centre d'administration Microsoft pour différentes raisons :

- la gestion des licences ;
- l'amélioration des produits lors de la détection de problèmes ;
- les fonctionnalités types « expériences connectées » *(connected experiences) ;*
- l'inventaire des plug-ins et des macros ;
- le reporting des actions de partage et de communication.

Cette analyse permet également aux services Office 365 de faire des recommandations personnalisées aux utilisateurs (typiquement dans Delve).

Les fonctionnalités types *connected experiences* sont proposées dans Word, PowerPoint ou Excel pour aider les utilisateurs : par exemple Word intègre un assistant pour faire un résumé du document ; PowerPoint Designer présente automatiquement des propositions de présentation ; Excel a aussi un module « Ideas » qui exploite les données pour mieux les traiter ou les restituer.

Il y a deux types d'expériences connectées :

- **expériences qui analysent le contenu pour fournir des recommandations ou suggestions ;**
- **expériences qui téléchargent du contenu complémentaire, proposé aux utilisateurs pour améliorer leurs documents.**

Les compléments des applications de la suite bureautique sont développés par Microsoft ou également par des éditeurs tiers. Donc si le paramétrage sécurité Office 365 le permet, des données peuvent aussi être envoyées à l'éditeur du complément installé par un utilisateur.

Exemple

Un nouveau complément développé par une société partenaire de Microsoft est installé sur les postes des utilisateurs. Le processus Microsoft de vérification du complément n'a pas détecté de problème, mais l'éditeur a subi une intrusion dans ses systèmes permettant une extraction des données envoyées par les utilisateurs du complément. Les données sensibles peuvent ainsi être récupérées.

Mesures

- **CMH-5 Durcissement des configurations des services bureautique (expériences connectées, télémétrie…)**

III.6.3. RB04 Non-maîtrise des compléments

Un utilisateur peut être induit en erreur et être invité à utiliser un complément Microsoft 365 Apps malveillant. Ce complément pourrait ainsi récupérer ou altérer les données de l'utilisateur.

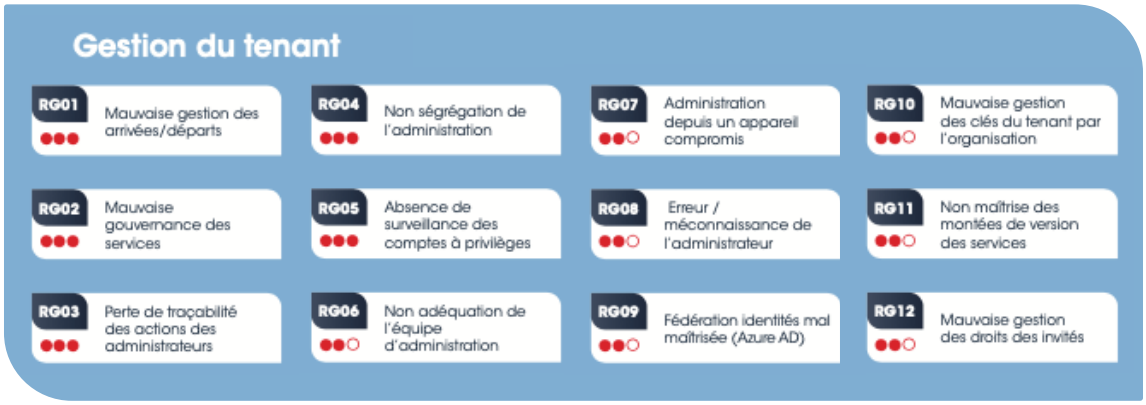
Exemple

Une utilisatrice reçoit un message l'invitant à tester la nouvelle application facilitant la réservation de réunions. En cliquant, elle installe depuis l'Office Store, un complément Outlook utilisant un accès en lecture et écriture sur sa boîte aux lettres. Elle valide machinalement et donne un contrôle complet à sa messagerie.

Mesures

- **CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité**
- **CMI–6 Mettre en place un processus de gestion des services tiers**

III.7. Gestion du locataire (tenant)



RG : Risque Gestion

III.7.1. RG01 Mauvaise gestion des départs et des arrivées

Une mauvaise gestion des utilisateurs, en particulier lorsqu'ils quittent l'organisation peut entraîner des accès illégitimes à des données du fait de la conservation des accès. Ce risque est encore plus important pour les administrateurs, qui pourraient conserver leurs privilèges lorsqu'ils changent de poste ou qu'ils quittent l'organisation.

Plus d'informations

Ce risque concerne également la gestion de la propriété des espaces de stockage (SharePoint/ OneDrive) qui doit prévoir les changements nécessaires à la modification/suppression d'un compte qui possède un espace Teams, SharePoint et une politique pour déterminer le devenir des données d'un espace personnel OneDrive.

Un corollaire à ce risque est l'explosion du nombre de licences du fait de la non-suppression régulière des comptes des personnes ayant quitté l'organisation.

Le processus doit prévoir la protection des données personnelles, notamment pour les répertoires OneDrive personnels. Les mêmes principes d'effacement des répertoires personnels d'un serveur de fichiers hébergé en interne doivent s'appliquer.

Une bonne pratique peut être l'envoi systématique d'un message d'alerte au manager pour qu'il décide des actions à mener sur les espaces concernés lors du départ ou de la mutation d'un de ses collaborateurs.

Exemple

Un employé quitte l'organisation pour aller à la concurrence. Son compte n'est pas désactivé et sa licence Office 365 n'est pas supprimée. Il continue d'accéder à toutes les données concurrentielles stockées sur Office 365.

Le départ d'un stagiaire ou d'un prestataire de l'organisation doit être anticipé pour que les fichiers de son espace personnel soient recopiés dans un espace partagé. De même la propriété des espaces partagés doit être transférée à un autre membre de l'équipe.

Mesures

- **CMI-2 Mettre en place une gestion des arrivées/départs**
- **CMP-4 Définir un processus de récupération des données**
- **CMG-3 Définir une stratégie de rétention des données**

III.7.2. RG02 Mauvaise gouvernance des services

L'adhésion à Office 365 donne accès à une multitude de services et d'applications. Chaque organisation est amenée à déterminer les services qu'elle souhaite mettre à disposition de ses utilisateurs.

Le choix et la configuration d'applications ou services sont un travail récurrent car Microsoft met régulièrement à disposition de nouveaux services. Selon les services, ils peuvent être activés par défaut et par conséquent accessibles aux utilisateurs sans que les risques et les usages aient été revus au préalable. Une mauvaise gestion des nouveaux services peut poser un problème si leur usage se développe sans une configuration sécurité adaptée aux enjeux de l'organisation.

Pour les grosses organisations, la gestion de cette gouvernance est rendue plus complexe par la multiplicité des locataires (tenants) de l'organisation et la multiplicité des équipes d'administration. Les choix sécurité de l'organisation doivent si possible être reproduits de façon cohérente.

Il faut cependant faire attention aux impacts d'une désactivation tardive d'un service qui a commencé à être utilisé par certains utilisateurs.

Exemple

Microsoft propose un nouveau service qui intéresse fortement les équipes marketing pour traiter des données clients, mais ce service n'est pas supporté dans un premier temps sur les plateformes Microsoft européennes. L'usage de ce nouveau service nécessite donc une localisation des données en dehors de l'Europe, ce qui peut être contraire à la politique de données de l'organisation.

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**
- **CMG-6 Mettre en place une gestion stricte des licences**
- **CMG-7 Mettre en place un processus de sélection et de configuration des services**
- **CMH-6 S'outiller pour mieux gérer son locataire (tenant) (pour grandes organisations)**

III.7.3. RG03 Perte de traçabilité des actions des administrateurs

Afin de détecter des comportements illicites ou de remonter à la cause d'un incident, il est nécessaire de tracer les actions des utilisateurs et des administrateurs.

L'organisation doit s'assurer qu'elle conserve accès aux traces des actions des administrateurs sur une plage de temps suffisante.

Plus d'informations

Par défaut, la journalisation des actions des utilisateurs n'est pas activée. Une action administrateur doit être réalisée dans le centre de sécurité et de conformité.

Les durées de conservation des logs dépendent du niveau de licence de l'organisation (entre 90 et 365 jours). Pendant ce laps de temps, les journaux *(unified audit logs)* sont disponibles dans les centres de sécurité et de conformité.

Afin d'obtenir une durée de conservation suffisante, ces journaux peuvent également être exportés vers un espace de stockage tiers ou SIEM. Pour cela, les journaux sont exportables au travers des API Management ou *via* des connecteurs spécifiques.

Il est également opportun de noter que Microsoft fournit des journaux plus détaillés sur certaines actions administrateur (comme l'accès aux boîtes aux lettres) avec les licences les plus élevées.

Exemple

Dans le cadre d'une compromission d'un compte administrateur, il est nécessaire de déterminer quelles actions ont été effectuées. Les actions ayant été réalisées il y a plus de 90 jours, les journaux ne sont pas disponibles.

Mesures

- CMI–3 Mettre en place une revue des comptes et privilèges
- CMD-1 Monitorer les modifications de configuration

III.7.4. RG04 Non-ségrégation de l'administration

Par défaut, la personne ouvrant le service Office 365 pour l'organisation hérite du rôle « Administrateur général ». Ce niveau d'administration lui confère la possibilité de modifier l'ensemble des paramètres du locataire (tenant) et la capacité d'accéder à toutes les données. Il peut également nommer à son tour d'autres administrateurs pour déléguer l'administration des services.

Lors de l'attribution de rôles d'administration, il est alors nécessaire d'appliquer le principe du moindre privilège afin de limiter l'exposition des services et garantir une hygiène dans le locataire (tenant).

Plus d'informations

Le modèle d'administration d'Office 365 s'appuie sur deux niveaux :

- rôles Azure AD pour l'administration des services ;
- rôles RBAC pour l'administration des objets et des politiques au sein des services.

À l'heure de l'écriture de ce document, il existe plus de 60 rôles Office 365 et Azure AD. Il est préférable d'attribuer un ou plusieurs de ces rôles afin de ne donner que les droits nécessaires pour les tâches à accomplir par l'administrateur.

Les rôles principaux Azure AD les plus couramment utilisés sont rappelés ci-dessous :

- administrateur général ;
- administrateur SharePoint ;
- administrateur Teams ;
- administrateur Exchange Online ;
- administrateur de sécurité ;
- administrateur de conformité
- administrateur d'utilisateurs.

Les rôles ci-dessus permettent notamment d'avoir une répartition des rôles et des responsabilités entre la production et les équipes sécurité.

Une gestion plus fine de ces rôles d'administration est désormais possible avec la création de rôles personnalisés selon les besoins de l'organisation, ou les rôles RBAC. Ces derniers sont notamment disponibles dans Exchange Online, Intune, les centres de sécurité et de conformité, les outils de sécurité.

La liste des rôles étant régulièrement mise à jour, il est possible de trouver la liste exhaustive des rôles d'administration avec les permissions associées, à la page suivante :

https://docs.microsoft.com/fr-fr/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide

Les rôles d'administration les plus courants à la date de publication de ce document sont :

Administrateur Exchange/Exchange admin	Attribuez le rôle d'administrateur Exchange aux utilisateurs qui doivent afficher et gérer les boîtes aux lettres de messagerie de vos utilisateurs, les groupes Microsoft 365 et Exchange Online. Les administrateurs Exchange peuvent aussi : • **Récupérer des éléments supprimés dans la boîte aux lettres d'un utilisateur** • **Configurer les délégués « Envoyer en tant que » et « Envoyer de la part de »**
Administrateur global/Global admin	Attribuez le rôle d'administrateur général aux utilisateurs qui doivent avoir un accès global à la plupart des fonctionnalités de gestion et des données dans les services Microsoft Online. Le fait de donner un accès global à un grand nombre d'utilisateurs représente un risque pour la sécurité et nous vous recommandons de n'avoir que 2 à 4 administrateurs généraux. Seuls les administrateurs généraux peuvent : • **Réinitialiser les mots de passe pour l'ensemble des utilisateurs** • **Ajouter et gérer des domaines** Remarque : la personne qui s'est inscrite aux services Microsoft Online devient automatiquement un administrateur général.
Lecteur général/Global reader	Attribuez le rôle de lecteur global aux utilisateurs qui doivent afficher les fonctionnalités et paramètres d'administration dans des centres d'administration que l'administrateur général peut afficher.
Administrateur de groupes/Groups admin	Attribuez le rôle d'administrateur de groupes aux utilisateurs qui doivent gérer tous les paramètres de groupes dans les centres d'administration, y compris le centre d'administration Microsoft 365 et le portail Azure Active Directory. Les administrateurs de groupe peuvent : • **Créer, modifier, supprimer et restaurer les groupes Microsoft 365** • **Créer et mettre à jour les stratégies de création, d'expiration et de désignation de groupes** • **Créer, modifier, supprimer et restaurer des groupes de sécurité Azure Active Directory**
Administrateur du support technique/Helpdesk admin	Attribuez le rôle d'administrateur du support technique aux utilisateurs qui doivent effectuer les opérations suivantes : • **Réinitialiser des mots de passe** • **Forcer les utilisateurs à se déconnecter** • **Gérer des demandes de service** • **Surveiller l'état d'intégrité des services**

	Remarque : l'administrateur du support technique peut uniquement aider des utilisateurs sans rôle d'administrateur et les utilisateurs ayant ces rôles : lecteur d'annuaire, invités hôtes, administrateur du support technique, lecteur de centre de messages et lecteur de rapports.
Administrateur d'applications Office/Office Apps admin	Attribuez le rôle d'administrateur d'applications Office aux utilisateurs qui doivent effectuer les opérations suivantes : • **Utiliser le service de stratégie cloud Office pour créer et gérer des stratégies basées sur le cloud pour Office** • **Créer et gérer des demandes de service** • **Gérer le contenu des nouveautés que les utilisateurs peuvent afficher dans les applications Office** • **Surveiller l'état d'intégrité des services**
Administrateur de service/Service admin	Attribuez le rôle d'administrateur de service à un rôle supplémentaire pour les administrateurs ou les utilisateurs dont le rôle n'inclut pas les éléments suivants, bien qu'ils doivent effectuer les opérations suivantes : • **Ouvrir et gérer des demandes de service** • **Afficher et partager des billets du centre de messages**
Administrateur SharePoint/SharePoint admin	Attribuez le rôle d'administrateur SharePoint aux utilisateurs qui doivent accéder et gérer le centre d'administration SharePoint Online. Les administrateurs SharePoint peuvent également : • **Créer et supprimer des sites** • **Gérer les collections de sites et les paramètres globaux de SharePoint**
Administrateur du service Teams/Teams service admin	Attribuez le rôle d'administrateur du service Teams aux utilisateurs qui doivent accéder et gérer le centre d'administration Teams. Les administrateurs du service Teams peuvent également : • **Gérer des réunions** • **Gérer les ponts de conférence** • **Gérer tous les paramètres à l'échelle de l'organisation, notamment la fédération, la mise à jour de Teams et les paramètres du client Teams**
Administrateur d'utilisateurs/User admin	Attribuez le rôle d'administrateur d'utilisateurs aux ceux qui doivent effectuer les opérations suivantes pour l'ensemble des utilisateurs : • **Ajouter des utilisateurs et des groupes** • **Attribuer des licences** • **Gérer la plupart des propriétés des utilisateurs** • **Créer et gérer les affichages utilisateurs** • **Mettre à jour les stratégies d'expiration des mots de passe**

	• **Gérer des demandes de service** • **Surveiller l'état d'intégrité des services** L'administrateur d'utilisateurs peut également effectuer les actions suivantes pour les utilisateurs qui ne sont pas administrateurs et pour ceux auxquels les rôles suivants sont attribués : lecteur de répertoire, inviteur d'invités, administrateur du support technique, lecteur du centre de messages, lecteur de rapports : • **Gérer les noms d'utilisateur** • **Supprimer et restaurer des d'utilisateurs** • **Réinitialiser des mots de passe** • **Forcer les utilisateurs à se déconnecter** • **Mettre à jour les clés d'appareils (FIDO)**

Exemple

Afin de favoriser l'adoption des entités, une organisation attribue des droits d'administration élevés à chacun des responsables IT locaux. Une responsable IT décide de modifier les conditions d'accès au locataire (tenant) pour son périmètre, mais impacte l'ensemble des entités.

Mesures

- CMG-2 Définir un modèle de rôles sécurisé
- CMI–3 Mettre en place une revue des comptes et privilèges
- CMG-5 Former les administrateurs et les développeurs

III.7.5. RG05 Absence de surveillance des comptes à privilèges

Les connexions et les actions des administrateurs Office 365 doivent être tracées afin de remonter des alertes sur leurs activités. En particulier, le rôle *global admin* doit faire l'objet d'une surveillance spécifique. Le traitement des alertes doit être réalisé par les équipes Office 365 et sécurité. L'administrateur doit avoir connaissance du déclenchement d'une alerte afin de le sensibiliser et le responsabiliser.

Ce risque est à prendre en compte dans la gestion globale de l'administration et dans la surveillance des systèmes d'information (SOC, RSSI…). Ce risque augmente par l'usage de comptes génériques (ou non individuels) pour administrer Office 365.

Exemple

Un administrateur ayant le rôle « global admin » attribue des privilèges à un utilisateur sans application des règles de validation. La surveillance permet de détecter cette action et de déclencher une alerte. Le traitement de l'alerte contribue à limiter le non-respect des règles.

Un administrateur messagerie s'attribue des droits de gestion d'une boîte aux lettres. L'absence de surveillance peut engendrer le maintien de ces droits au-delà des actions à réaliser.

Plus d'information :

Il est possible de configurer Office 365 pour envoyer automatiquement une alerte lorsqu'un utilisateur se voit attribuer des autorisations d'administration dans Exchange Online.

https://docs.microsoft.com/fr-fr/microsoft-365/compliance/alert-policies?view=o365-worldwide

Mesures

- CMI–3 Mettre en place une revue des comptes et privilèges
- CMD-1 Monitorer les modifications de configuration

III.7.6. RG06 Non-adéquation de l'équipe d'administration

Le passage au cloud n'est pas nécessairement synonyme de disparition des équipes d'administration, telle qu'imaginée par les équipes de direction. Certes, les équipes historiquement dédiées à l'administration des serveurs et des applications on-premises voient leur périmètre diminuer ; mais de nouveaux besoins sont créés pour gérer les nouveaux services de collaboration et de communication d'une plateforme telle que Office 365.

La taille de l'équipe d'administration doit être adaptée à l'organisation, en fonction de la volumétrie des demandes de support et l'ambition de la feuille de route. Il n'est en effet pas souhaitable d'avoir une équipe réduite à deux ou trois personnes pour gérer la construction et le maintien d'un locataire (tenant) de plus de 100 000 utilisateurs.

Exemple

Une équipe d'administration Office 365 trop peu nombreuse n'est pas en mesure de traiter les différents projets autour de l'environnement de travail. Cela peut conduire à retarder certaines activités. Afin de répondre aux demandes, des droits d'administration sont attribués à des personnes non expertes qui ne maîtrisent pas la portée de leurs actions.

Mesures

- CMG-5 Former les administrateurs et les développeurs
- CMI–1 Mettre en place une authentification renforcée

III.7.7. RG07 Administration depuis un appareil compromis

Un administrateur se connectant aux services d'administration *via* un portail Web Office 365 ou PowerShell depuis un appareil compromis donne la possibilité à un attaquant de récupérer des informations ou d'effectuer des modifications sur la configuration du locataire (tenant).

Exemple

Un administrateur se fait compromettre son poste de travail par l'intermédiaire d'un malware reçu par la messagerie. Ce même poste étant utilisé pour l'administration Office 365, lors de la connexion de l'administrateur à Office 365, le malware utilise l'identité et le mot de passe de l'administrateur pour créer un compte administrateur du locataire (tenant) et envoyer les éléments d'authentification à l'attaquant.

Mesures

- CMG-5 Former les administrateurs et les développeurs
- CMH-10 Mettre en œuvre des stations d'administration sécurisées et dédiées (PAW)
- **CMI–5 Maîtriser les appareils autorisés à accéder à Office 365**
- CMP-6 Mettre en place le contrôle d'accès conditionnel

III.7.8. RG08 Erreur/méconnaissance de l'administrateur

Un administrateur est par définition un utilisateur ayant des privilèges élevés sur le locataire (tenant), en particulier sur les paramétrages des services et sur les données des utilisateurs finaux.

En cas d'erreur, une action d'administration peut entraîner l'exposition, la modification ou la suppression des données hébergées, provoquer une indisponibilité ou encore amoindrir l'expérience utilisateur.

Exemples

- Un administrateur fait des tests sur les politiques de rétention sur le locataire (tenant) de production. Par erreur, il supprime l'intégralité des messages Teams.
- Un administrateur effectue une tâche d'administration sur Exchange Online. Il se rend alors compte que la portée de son acte est plus large que prévu initialement, car il n'avait pas eu connaissance que Microsoft avait modifié le paramètre en question.

Mesures

- CMG-5 Former les administrateurs et les développeurs
- CMG-8 Maîtriser les transferts de données (Réversibilité)
- CMH-7 Documenter la gestion du locataire (tenant)
- CMD-1 Monitorer les modifications de configuration

III.7.9. RG09 Fédération d'identités mal maîtrisée (Azure AD)

La plupart des grandes organisations utilisent toujours un référentiel d'identité Active Directory en interne tout en souhaitant offrir une expérience de SSO avec Office 365. L'outil Azure AD Connect (disponible gratuitement) permet de gérer à la fois la synchronisation entre l'annuaire Active Directory interne et Azure Active Directory – le référentiel des identités Office 365 dans le cloud – et la fonction de SSO. Trois solutions sont disponibles :

- **la synchronisation de hashs des mots de passe (Password Hash Sync) ;**
- **l'authentification directe qui redirige les authentifications vers l'Active Directory interne (Pass Through Authentication) ;**
- **la fédération d'identités qui nécessite de déployer des serveurs de fédération en interne, mais accessibles depuis l'extérieur.**

Même si la solution de synchronisation des mots de passe est de loin la plus déployée, la fédération d'identités reste utilisée par certaines organisations disposant d'une infrastructure de fédération. La fonction d'authentification est critique car, sans elle, l'accès à Office 365 n'est plus possible. Dans le cas de l'utilisation de la fédération, l'infrastructure doit être hautement disponible ce qui implique une sécurisation (mesure anti-DDoS, etc.) et un dimensionnement adapté au nombre d'authentifications, une protection de l'accès au service par une administration rigoureuse et une surveillance de l'état du service.

Exemple

L'infrastructure de fédération de l'organisation est sous-dimensionnée. Suite à une attaque en déni de service, l'infrastructure n'est plus disponible et ne permet plus aux utilisateurs d'accéder à leurs données.

Mesures

- CMI–4 : Assurer la disponibilité de l'authentification en mode fédéré

III.7.10. RG10 Mauvaise gestion des clés du locataire (tenant) par l'organisation

Les données au repos sur les serveurs de Microsoft sont protégées nativement par un chiffrement BitLocker et Distributed Key Manager (DKM). Ce chiffrement, appliqué sur les serveurs, est activé par défaut quel que soit le niveau de licence du locataire (tenant).

En option, Microsoft propose un chiffrement au niveau applicatif. Celui-ci, appelé « chiffrement des services avec clé client » (clé client ou *Customer Key*), couvre les services Exchange Online, SharePoint Online, OneDrive for Business et Teams. Cette fonctionnalité permet aux clients qui seraient soumis à des contraintes réglementaires spécifiques de démontrer leur capacité à utiliser leurs propres clés pour chiffrer les données au repos de ces services Office 365.

Lorsque le client veut imposer au service d'utiliser ses propres clés, il doit lui spécifier d'utiliser des clés stockées dans Azure Key Vault. Ces clés sont générées par le client dans Azure Key Vault de manière logicielle ou en s'appuyant sur un HSM du centre de données. Le client peut également choisir de générer ses clés générées dans son propre HSM on-premise et de les transférer vers le HSM du centre de données (ce mécanisme est désigné sous l'acronyme *Bring You Own Key,* ou BYOK).

Pour plus d'information, voir le livre blanc dédié au sujet (FAQ Bring Your Own Key et Azure Key Vault)	https://www.microsoft.com/fr-fr/download/details.aspx?id=57310
Pour la liste des fabricants de HSM supportés, veuillez consulter le lien	https://docs.microsoft.com/en-us/azure/key-vault/keys/hsm-protected-keys#supported-hsms

Sachant que la gestion des clés de chiffrement est alors de la responsabilité du client, la suppression des clés de chiffrement dans Azure Key Vault (par une erreur de manipulation ou un acte malveillant intentionnel) peut entraîner une indisponibilité des données contenues dans les services Office 365 concernés.

Manage Customer Key	https://docs.microsoft.com/en-us/microsoft-365/compliance/customer-key-manage?view=o365-worldwide

Note :

La fonctionnalité optionnelle de gestion de la clé client n'est accessible qu'aux locataires (tenants) munis de l'offre proposée dans Office 365 E5, M365 E5, M365 E5 conformité et M365 E5 information protection & gouvernance.

https://docs.microsoft.com/fr-fr/microsoft-365/compliance/customer-key-set-up?view=o365-worldwide#before-you-set-up-customer-key

Exemple

Une organisation implémente la fonctionnalité Customer Key. À la suite d'une erreur d'administration, elle n'a plus accès à la clé et perd potentiellement l'accès à ses données.

Mesure

- CMP-8 Respecter les bonnes pratiques liées à l'utilisation de Customer Key

III.7.11. RG11 Non-maîtrise des montées de version des services

Office 365 étant une solution SaaS, les différents services sont régulièrement mis à jour par Microsoft *via* l'ajout, la modification ou la suppression des fonctionnalités. Une absence de durcissement ou d'anticipation pourrait avoir des conséquences comme une exposition des données hébergées, une non-conformité réglementaire ou un impact des cas d'usages métiers.

Plus d'informations

Ces évolutions peuvent être regroupées en trois catégories :

- évolution d'un service de la plateforme – Ces évolutions sont poussées par Microsoft en continu, sans maîtrise granulaire côté locataire (tenant) ;
- évolution des applications « clients lourds » – La suite Microsoft 365 Apps (incluant Word, Excel, PowerPoint) est également régulièrement mise à jour. De même que pour les autres services Office 365, les évolutions fonctionnelles pourraient impacter les utilisateurs en cas d'apparition de nouvelles fonctionnalités ou d'absence de support des fonctionnalités natives ou ajoutées (ex. : macro VBA) existantes. Le locataire (tenant) a ici la possibilité de maîtriser les montées de version *via* une publication mensuelle, semi-annuelle ou annuelle ;
- évolution des applications « client mobile » – Les applications iOS et Android de la suite Office reçoivent également leurs lots de mise à jour. En revanche, les évolutions sont poussées en continu par Microsoft sans aucun contrôle possible par le locataire (tenant) : les utilisateurs sont libres de mettre à jour ou non leurs applications mobiles.

https://www.microsoft.com/en-us/microsoft-365/roadmap

Mesures

- **CMG-1 Veiller à la mise à jour Office 365**

III.7.12. RG12 Mauvaise gestion des droits donnés aux invités

Office 365 permet à des personnes extérieures au locataire (tenant) de venir collaborer sur les données ou d'utiliser une application. Ces utilisateurs, appelés « invités », peuvent être ajoutés à collaborer sur un fichier, un espace défini (Groupe Office 365, Teams, site SharePoint, etc.) ou encore au niveau du locataire (tenant). Ces personnes invitées bénéficient par défaut d'accès à des données sans limite de temps.

Il est important de noter que l'authentification de ces invités sera portée par leur locataire (tenant) d'origine dans le cas de comptes Office 365 existants ou par leur fournisseur d'identité dans le cas général.

Exemple

Un consultant est invité dans un Groupe Office 365 le temps d'une mission, afin de collaborer sur des documents. Si ses droits ne lui sont pas retirés, il conservera un accès à l'ensemble des documents actuels et à venir.

Un employé invite son compte personnel sur une ressource pour ne pas être soumis aux règles de l'organisation, quant à ses identifiants et ses terminaux.

Mesures

- CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité

- CMI-2 Mettre en place une gestion des arrivées/départs
- CMI-7 Implémenter un cycle de vie des utilisateurs invités
- CMP-3 Limiter les droits d’accès aux documents partagés en externe
- CMP-6 Mettre en place le contrôle d’accès conditionnel
- CMD-3 Monitorer les accès aux données

III.8. Lois

RL : Risque Lois

III.8.1. RL01 Non-conformité réglementaire

En tant que client, il est nécessaire de s'assurer que le passage à Office 365 se fasse en respect des exigences réglementaires. Ceci passe d'abord par une connaissance précise des exigences réglementaires qui s'appliquent à sa propre organisation et des rôles et responsabilités dans la relation de sous-traitant qui va s'appliquer avec Microsoft pour sa solution SaaS Office 365.

Concernant la France, la protection des données est régie principalement par la loi Informatique et Libertés et le Règlement général sur la protection des données (RGPD) ainsi que l'arrêt récent de la Cour Européenne de Justice en juillet 2020 dit SHREMS II. À ces principales réglementations, qui concernent toutes les organisations, s'ajoutent de nombreuses réglementations sectorielles. On peut citer, pour les plus importantes, la directive européenne NIS (Network & Information Security) pour les OSE (opérateurs de services essentiels, environ 500 sociétés), la loi de programmation militaire pour les OIV (opérateurs d'intérêts vitaux, environ 200 sociétés), mais aussi les réglementations sur les données de Santé, entre autres.

Office 365 est un service SaaS qui opère sur les données des clients et la question principale qui se pose est de savoir si les réglementations qui s'appliquent à votre organisation vous permettent de stocker tout ou partie de vos données et sous quelles conditions de protection. On peut formuler plus précisément :

- le fait de choisir un fournisseur de cloud américain m'impose-t-il des contraintes particulières d'un point de vue réglementaire ?
- est-il nécessaire de mettre en place des mesures de protection particulières selon les données qui seront hébergées ?
- puis-je héberger tout type de données, quelle que soit leur sensibilité tout en restant conforme ? (Indépendamment des résultats d'une analyse de risques qui prendrait en compte d'autres facteurs non liés à la réglementation)

Mesures

- CMG-3 Définir une stratégie de rétention des données
- CMP-1 Classifier les documents et messages
- CMP-2 Protéger les informations sensibles par chiffrement
- CMD-3 Monitorer les accès aux données
- CMR-1 Comprendre les exigences de conformité du fournisseur Microsoft
- CMR-2 Prendre en compte des réglementations nationales spécifiques et sectorielles
- CMR-3 Comprendre les risques liés aux réglementations et aux engagements du fournisseur de cloud

IV. Comment sécuriser son usage Office 365

Ce chapitre présente les principales mesures permettant de réduire les risques présentés dans le chapitre III.

Elles sont regroupées selon les six familles suivantes :

Mesures de gouvernance		**Complexité de mise en oeuvre**
CMG-1	Veiller à la mise à jour Office 365	Simple
CMG-2	Définir un modèle de rôles sécurisé	Simple à complexe
CMG-3	Définir une stratégie de rétention des données	Moyen
CMG-4	Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	Moyen à complexe
CMG-5	Former les administrateurs et les développeurs	Moyen
CMG-6	Mettre en place une gestion des licences stricte	Simple
CMG-7	Mettre en place un processus de sélection et de configuration des services	Moyen à complexe
CMG-8	Maîtriser les transferts de données (Réversibilité)	Moyen à complexe
Mesures d'hygiène et bonnes pratiques		
CMH-1	S'équiper contre les codes malveillants	Simple
CMH-2	Durcissement des configurations des services de collaboration	Moyen
CMH-3	Durcissement des configurations des services de messagerie	Moyen
CMH-4	Durcissement des configurations des développements	Moyen
CMH-5	Durcissement des configurations des services bureautique	Moyen
CMH-6	S'outiller pour mieux gérer son locataire (tenant) (pour grosses entités)	Moyen à complexe
CMH-7	Documenter la gestion du locataire (tenant)	Simple à moyen
CMH-8	Faciliter le travail en mode déconnecté	Simple à moyen
CMH-9	Surveiller les performances des infrastructures d'accès et augmenter la bande passante si nécessaire	Simple
CMH-10	Mettre en œuvre des stations d'administration sécurisées et dédiées (PAW)	Complexe
CMH-11	Déterminer l'indisponibilité effective du service Office 365	Moyen
Mesures de gestion des identités et des accès à Office 365		
CMI–1	Mettre en place une authentification renforcée	Simple à moyen
CMI–2	Mettre en place une gestion des arrivées/départs	Simple à complexe
CMI–3	Mettre en place une revue des comptes et privilèges	Moyen à complexe
CMI–4	Assurer la disponibilité de l'authentification en mode fédéré	Moyen
CMI–5	Maîtriser les appareils autorisés à accéder à Office 365	Moyen à complexe
CMI–6	Mettre en place un processus de gestion des services tiers	Moyen à complexe

CMI–7	Implémenter un cycle de vie des utilisateurs invités (création, modification, suppression)	Simple à moyen
Mesures de protection de l'information stockée dans Office 365		
CMP-1	Classifier les documents et messages	Simple à complexe
CMP-2	Protéger les informations sensibles par chiffrement	Simple
CMP-3	Limiter les droits d'accès aux documents partagés en externe	Simple à moyen
CMP-4	Définir un processus de récupération des données	Simple
CMP-5	Gérer les applications avec un outil de gestion des applications mobiles	Moyen à complexe
CMP-6	Mettre en place le contrôle d'accès conditionnel	Moyen à complexe
CMP-7	Interdire la synchronisation des données depuis les appareils non gérés	Simple
CMP-8	Respecter les bonnes pratiques liées à l'utilisation de Customer Key	Complexe
Mesures de détection des événements sécurité Office 365		
CMD-1	Monitorer les modifications de configuration	Moyen à complexe
CMD-2	Monitorer les usages	Moyen à complexe
CMD-3	Monitorer les accès aux données	Moyen à complexe
Mesures de protection contre les risques réglementaires		
CMR-1	Comprendre les exigences de conformité du fournisseur Microsoft	Simple
CMR-2	Prise en compte des réglementations nationales spécifiques et sectorielles	Moyen à complexe
CMR-3	Compréhension des risques liés aux réglementations et aux engagements du fournisseur de cloud	Simple

IV.1. Mesures de gouvernance

IV.1.1. CMG-1 Veiller à la mise à jour Office 365

La mise à jour régulière des produits Office 365 est une mesure organisationnelle qui nécessite un minimum de veille sur l'évolution des produits.

Avoir un suivi régulier du « Message Center » et de la « Roadmap » Microsoft Office 365	https://docs.microsoft.com/fr-fr/office365/admin/manage/stay-on-top-of-updates?view=o365-worldwide

Ce maintien suppose une vision globale des fonctionnalités utilisées par les utilisateurs de son organisation pour pouvoir les confronter aux modifications prévues par Microsoft.

Pour les utilisateurs disposant d'applications métiers, de compléments ou de macros qui sont essentiels pour l'entreprise	https://docs.microsoft.com/fr-fr/deployoffice/change-management-for-office-365-clients

La veille doit être organisée dans un cadre de gouvernance permettant la prise de décision.

Vidéo mensuelle expliquant les évolutions d'Office 365	https://www.youtube.com/channel/UCc3pNIRzIZ8ynI38GO6H01Q

Il faut communiquer auprès des utilisateurs finaux les mises à jours impactantes qui vont être réalisées sur Office365.

L'organisation en cercles de personnes permet de rendre le processus efficace et peu coûteux :

- le premier cercle comprend quelques personnes IT qui bénéficient des changements au fur et à mesure de leur publication. Si aucun problème n'est détecté, les changements peuvent être opérés sur le deuxième cercle ;
- le deuxième cercle comprend un panel de personnes représentatif des utilisateurs de l'organisation (métier et IT). Ils bénéficient des changements à intervalles réguliers en avance de phase pour s'assurer du bon fonctionnement des applications et des usages propres à l'organisation. Si aucun problème n'est détecté, les changements peuvent être déployés sur le troisième cercle (autres utilisateurs n'étant ni dans le premier ni dans le second cercle) ;
- le déploiement du troisième cercle peut être organisé par vague pour prévenir une éventuelle saturation du support utilisateur.

Le passage de changement entre cercles peut faire l'objet de revues formelles selon la gouvernance définie. Les modifications importantes du locataire (tenant) peuvent se faire à quatre-yeux, en ne communiquant pas l'intégralité des mots de passe aux administrateurs.

IV.1.2. CMG-2 Définir un modèle de rôles sécurisé

Sur Office 365, trois types d'utilisateurs ont chacun des niveaux de privilèges différents : **les administrateurs, les utilisateurs internes et les invités** (externes invités à collaborer par exemple sur un fichier au sein d'un site SharePoint ou Teams).

Les permissions des administrateurs dans Office 365 (et Azure AD) ont par conception une portée globale et les centres d'administration individuels sont utilisés pour restreindre les autorisations.

Il est possible de déléguer les rôles des administrateurs et pour cela Office 365 propose de nombreux rôles d'administration par défaut. Les petites structures n'ont pas besoin d'avoir de tels droits d'administration distribués et ont tendance à être moins granulaires.

Rôles d'administration par défaut	https://docs.microsoft.com/fr-fr/microsoft-365/admin/add-users/about-admin-roles?view=o365-worldwide#all-roles

Les administrateurs Office 365 sont par défaut membres du groupe *Tenant Global Administrator* et possèdent tous les droits. Un *Tenant Global Administrator* peut se donner le droit de lire la boîte aux lettres de n'importe quel utilisateur ou bien peut réinitialiser le mot de passe de n'importe quel utilisateur. Il est fortement conseillé de définir d'autres groupes moins privilégiés et d'affecter la plupart des administrateurs dans ces groupes en ne conservant que quelques *Tenant Global Administrators.*

	Tenant Global Administrator	Security Administrator	Compliance Administrator	Security Reader	Information Protection Administrator	Privileged Role Administrator	Intune Administrator	eDiscovery
Azure AD				Read Only		Grant Azure AD roles		
Microsoft 365 Security				View policies & reports				
Microsoft 365 Compliance								
Azure Information Protection								
Intune (RBAC)		Views only	Read Only	Read Only				
Cloud App Security (RBAC)			Read Only	Read Only				
Office 365 ATP								
Defender ATP Security Center (RBAC)				Read Only				
Azure ATP								
Security & Compliance Center (e-discovery + governance)		Security		Read Only				Custodians management
Privileged Identity Management		Read Only		Read Only				
Identity Protection Center				Read Only				
Secure Score				Read Only				

Exemple de matrice de rôles

IV.1.3. CMG-3 Définir une stratégie de rétention des données

Même si Office 365 est une application SaaS avec une capacité de stockage très importante, il est important de définir une stratégie de rétention des données en prenant en compte les éventuelles contraintes qui peuvent s'appliquer. Cette stratégie doit être communiquée et expliquée aux utilisateurs et des solutions doivent être définies pour permettre la conservation de données au-delà des délais prévus par l'organisation.

Dans le cas d'Office 365, il faut définir des délais selon les types de données, par exemple :

- la messagerie – durée de conservation d'une correspondance, pour un utilisateur actif ou plus particulièrement pour un utilisateur inactif ;
- les espaces personnels – durée de conservation des répertoires OneDrive, après le départ d'un utilisateur ;
- les espaces collaboratifs – durée de conservation en ligne d'un espace SharePoint ou Teams qui n'est plus modifié.

IV.1.4. CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité

L'utilisateur étant un maillon essentiel de la chaîne sécurité, il est essentiel de sensibiliser les utilisateurs du service Office 365 et en premier lieu, ceux manipulant des données sensibles pour l'organisation.

Cette sensibilisation doit permettre de présenter :

- les menaces spécifiques auxquels un utilisateur est exposé par l'usage de ce service (illustrées par des exemples pratiques concrets) ;
- les bonnes pratiques à respecter dans son utilisation quotidienne (accès au service depuis un appareil conforme aux Politiques de son organisation, respect des politiques relatives aux comptes d'accès, etc.) ;
- les conséquences d'autorisations accordées par erreur ou trop largement.

La sensibilisation des utilisateurs doit intégrer une explication de la charte et des conséquences pour l'organisation des mauvais comportements. A noter que certains contrats de travail intègrent des clauses de protection des données qui doivent être expliquer aux utilisateurs.
La sensibilisation concerne en particulier l'usage de la messagerie, même si Office 365 intègre de base une protection contre le phishing. Au-delà de la protection technique, l'éducation des utilisateurs est nécessaire avec un rappel des bonnes pratiques.

Comment Office 365 valide l'adresse de pour empêcher l'hameçonnage	https://docs.microsoft.com/fr-fr/microsoft-365/security/office-365-security/how-office-365-validates-the-from-address
Se protéger contre les techniques de phishing et d'autres formes de fraude en ligne	https://support.office.com/fr-fr/article/se-protéger-contre-les-techniques-de-phishing-et-d-autres-formes-de-fraude-en-ligne-be0de46a-29cd-4c59-aaaf-136cf177d593

IV.1.5. CMG-5 Former les administrateurs et les développeurs

Pour les populations ayant des privilèges, il est particulièrement important de s'assurer de leur niveau de compétences Office 365 afin d'éviter au maximum les erreurs de manipulation.

Les administrateurs devraient être formés et pour ceux qui ont le plus de droits, la validation des compétences par une certification est souhaitable. Il faut aussi s'assurer que les compétences sont maintenues par une formation continue et une veille sur la solution.

Les développeurs doivent aussi être formés à intégrer la sécurité dans leur développement. Selon l'organisation, les développeurs peuvent parfois avoir les mêmes droits que certains administrateurs pour qu'ils soient autonomes. Il faut dans ce cas les former comme les administrateurs pour qu'ils comprennent les conséquences de certains actes d'administration.

Enfin les utilisateurs ayant les accès aux fonctionnalités de développement (Powerapps, PowerBi…) doivent être sensibilisés, notamment aux contraintes réglementaires liées à la manipulation d'information à caractère personnel.

Cette formation peut inclure les bonnes pratiques de développement définies par l'organisation. Dans le cas de développements sous-traités, des clauses contractuelles peuvent être exigées sur les pratiques sécurité du sous-traitant.

IV.1.6. CMG-6 Mettre en place une gestion stricte des licences

Selon la taille de l'organisation, la gestion des licences peut être plus ou moins complexe. Il est, dans tous les cas, important d'exploiter les consoles Microsoft pour suivre les usages et s'assurer que les termes du contrat et les coûts induits restent dans les limites fixées par l'organisation.

Par exemple, dans le cas d'Office 365, le nombre de boîtes aux lettres est lié au nombre de comptes Azure AD, qui peut être lié, *via* Azure AD Connect, au nombre de comptes AD. Si les comptes ne sont pas correctement supprimés lors du départ d'un utilisateur, le nombre de boîtes aux lettres augmentera pour dépasser éventuellement les limites fixées.

Cela concerne en particulier les fonctionnalités d'Office 365 soumises à des licences spécifiques (selon les termes du contrat). Une licence attribuée à un utilisateur correspond en général à l'ajout de l'utilisateur dans un groupe spécifique. Si aucun contrôle n'est mis en place, le nombre d'utilisateurs va croître pour dépasser le nombre fixé de licences achetées.

La bonne pratique est de ne donner accès à un service Office 365 que :

- à une population contrôlée,
    - pour justifier le nombre de boîtes aux lettres et le nombre de répertoires personnels dans OneDrive ;
- depuis des appareils conformes à la politique de l'organisation,
    - pour limiter l'installation de logiciels soumis à licences sur des appareils non conformes (en fonction des termes contractuels).

IV.1.7. CMG-7 Mettre en place un processus de sélection et de configuration des services

Les services Office 365 évoluent régulièrement et un processus doit être mis en place pour analyser l'impact des nouveaux services ou des évolutions majeures de services existants. Ce processus doit permettre de déterminer si un nouveau service est utilisable par l'organisation et si c'est le cas, les paramètres sécurité de ce nouveau service.

Ce processus doit impliquer les experts Office 365 de l'organisation, éventuellement assistés du support Microsoft et les responsables sécurité de l'organisation.

IV.1.8. CMG-8 Maîtriser les transferts de données (réversibilité)

La mesure consiste à considérer service par service les moyens de transfert des données depuis le cloud et de les réinjecter dans un service similaire en interne.

Pour prendre quelques exemples, concernant le service de messagerie Exchange Online, la version Exchange existe et la procédure de récupération consiste à mettre en place une configuration Exchange hybride et effectuer un déplacement des boîtes aux lettres selon une procédure documentée.

Déplacement de boîtes aux lettres entre des organisations locales et Exchange Online dans des déploiements hybrides	https://docs.microsoft.com/fr-fr/exchange/hybrid-deployment/move-mailboxes

Pour OneDrive For Business, ou SharePoint Online, on pourra retransférer les fichiers vers des emplacements internes en automatisant cette tâche par exemple avec des scripts PowerShell qui s'appuient sur les API REST disponibles.

Utilisation des dossiers et des fichiers avec REST	https://docs.microsoft.com/fr-fr/sharepoint/dev/sp-add-ins/working-with-folders-and-files-with-rest

Les outils de la suite Office disponibles avec Microsoft 365 Apps for Enterprise (ex-Office 365 Pro-plus) en version click-to-run pourront être remplacés par leur pendant en version Office 2019, mais nécessiteront de s'appuyer sur une infrastructure interne pour le déploiement.

Pour d'autres services comme Teams, la tâche sera plus complexe car Teams joue un rôle d'unification entre différents services Office 365 et qu'il ne possède pas d'équivalent en version on-premise. De plus, les données de Teams sont réparties entre plusieurs stockages : BAL Exchange pour le chat, site SharePoint pour chaque canal, fichiers partagés durant des chats en 1-1 ou 1-many sont stockés dans OneDrive for Business, enregistrements vidéo stockés dans des blobs Azure puis encodés dans Stream, etc.). L'export des données est donc possible, mais le défi sera de trouver le ou les nouveaux outils qui devront remplacer fonctionnellement l'ensemble des services fournis par Teams et le moyen d'y réimporter les données.

Même si les données peuvent être récupérées, le retour-arrière engendrera un coût lié à la reconstruction d'une infrastructure pour mettre en place les services équivalents on-premises et à la migration elle-même.

IV.2. Mesures d'hygiène et bonnes pratiques

IV.2.1. CMH-1 S'équiper contre les codes malveillants

Il est recommandé que tous les appareils soient équipés d'une solution de protection contre les malwares. Ces solutions peuvent également assurer une protection réseau contre les Wifi malicieux, la vérification des vulnérabilités non patchées, etc., et s'appuient sur le cloud et le machine learning pour détecter des comportements suspects liés à des applications malicieuses. L'installation qui s'effectuera depuis le store de l'organisation peut être imposée par le MDM lors de la phase d'enregistrement.

Ces solutions connues sous la dénomination MTD (Mobile Threat Defense) peuvent s'interfacer avec les outils de MDM pour remonter des alertes et des informations sur l'état de santé de l'appareil.

Implémenter les solutions de protection incluses dans Office 365 et préconisées par Microsoft	https://docs.microsoft.com/en-us/office365/enterprise/office-365-malware-and-ransomware-protection
Appliquer les conseils de sécurité proposés par Microsoft concernant les infections par programme malveillant	https://docs.microsoft.com/en-us/windows/security/threat-protection/intelligence/prevent-malware-infection

IV.2.2. CMH-2 Durcissement des configurations des services de collaboration

Par défaut, certains usages des services de collaboration sont autorisés et lors de l'ouverture d'un service, il faut changer des paramètres pour réduire les risques.

Il est possible de configurer l'usage de OneDrive/SharePoint pour interdire les partages anonymes. À noter que Teams n'autorise pas un accès anonyme par défaut.

Il est possible de bloquer la synchronisation OneDrive pour certains types de fichiers ou depuis des ordinateurs non gérés par l'organisation.

Par défaut, les fichiers déposés sur OneDrive, SharePoint ou Teams sont analysés par l'antivirus SharePoint Online et ce mécanisme empêche le dépôt de fichiers malveillants (malware).

Les comptes « invités » ont accès aux fichiers/dossiers/équipes qui leur sont partagés. Il est possible de limiter cette fonctionnalité *via* la configuration générale.

La tendance est de protéger les documents, quels que soient leurs emplacements. Cette protection peut être paramétrée en deux étapes :

- la définition de la sensibilité du document, effectuée manuellement ou automatiquement ;
- l'application d'une stratégie de protection du document (chiffrement, limitation des accès…).

La configuration Teams autorise par défaut la création d'équipe regroupant des utilisateurs de l'organisation et des utilisateurs invités. Il est possible d'interdire cette capacité de création aux utilisateurs en mettant en place un processus de création par les administrateurs – ce qui n'est pas conseillé par Microsoft.

IV.2.3. CMH-3 Durcissement des configurations des services de messagerie

Pour limiter l'usurpation d'un domaine de messagerie, il faut configurer une politique SPF, DKIM et DMARC dans Office 365 et éventuellement dans les enregistrements DNS.

Explication des méthodes d'authentification messagerie	https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services

Les administrateurs messagerie peuvent durcir la configuration du service de messagerie, par exemple :

- limiter la capacité de délégation des boîtes aux lettres par les utilisateurs ;
- interdire les transferts automatiques de messages vers une boîte aux lettres externe à l'organisation ;
- limiter limiter erdire l'usage des anciens protocoles POP3 et IMAP.

Il est également possible de mettre en œuvre un service de filtrage complémentaire des liens et pièces jointes contenus dans les messages. Ces services, en coupure ou en mode API, proposent en particulier :

- le *sandboxing* des URL ;
- le *sandboxing* des pièces jointes ;
- des options de contrôle avancées SPF, DKIM et DMARC.

IV.2.4. CMH-4 Durcissement des configurations des développements

Afin limiter l'exposition des secrets utilisés par les applications développées en interne ou par les comptes de service, il est nécessaire d'en maîtriser le stockage et les accès.

La solution Azure Key Vault, mise à disposition par Microsoft, permet de stocker les secrets et d'y accéder en toute sécurité, et ainsi de gérer l'intégralité du cycle de vie des secrets :

- création ;
- conservation des secrets créés dans l'environnement ou en dehors ;
- gestion des accès (utilisation de l'authentification Azure AD) ;
- renouvellement et expiration.

Le niveau de sécurité associé à la solution Azure Key Vault peut être augmenté en l'associant avec un HSM on-premise.

Pour plus d'informations :

Présentation de la solution	https://docs.microsoft.com/fr-fr/azure/key-vault/general/overview

A noter, Azure Key Vault propose un connecteur intégré à Power Automate et Power Apps. Cela permet de protéger les secrets d'authentification pour les nouvelles applications nécessitant d'accéder au Microsoft Graph.

IV.2.5. CMH-5 Durcissement des configurations des services bureautique (expériences connectées, télémétrie…)

La protection des données privées de Microsoft 365 Apps for Enterprise doit être configurée selon les enjeux de chaque entité. Il faut distinguer :

- la configuration des services essentiels, correspondant aux données échangées avec Microsoft pour authentifier, configurer et autoriser (licence) l'usage de Microsoft 365 Apps for Enterprise. Ce service ne peut pas être désactivé par les administrateurs ;
- la configuration des données de diagnostic, utilisées pour remédier à un problème dans un produit. Ces données servent également à gérer les mises à jour. Les administrateurs peuvent désactiver partiellement ou complètement ce service ;
- la configuration des données utilisées dans les expériences connectées.

Données	Impact sécurité	Recommandation
Gestion des licences Office	Faible : information sur les licences déployées	Non configurable
Données de diagnostic	Positif : application automatique des correctifs sécurité Négatif : accès à de nouvelles fonctionnalités sans contrôle préalable	Activer les données de diagnostic suffisantes pour les MaJ Sécurité
Données tracking plug-ins et macros	Impact positif pour détecter d'éventuels plug-ins malicieux (ou macros malicieuses)	Activer les données de tracking
Données nécessaires aux traitements ATP	Positif : détection de lien contenu dans un document vers un site malicieux Négatif : pour analyser le contenu des documents, le système accède à l'information. Il y a donc un risque pour la confidentialité en fonction de la classification du document	Vérifier si d'autres mécanismes protègent le clic vers un lien malicieux
Données nécessaires aux services connectés	Positif : certains compléments augmentent la productivité des utilisateurs	Une analyse des risques doit être faite pour chaque complément autorisé

	Négatif : le contenu des documents est analysé pour des fonctionnalités peu utilisées *a priori*	

Essential Services for Office	https://docs.microsoft.com/en-us/deployoffice/privacy/essential-services
Required Diagnostic Data for Office	https://docs.microsoft.com/en-us/deployoffice/privacy/required-diagnostic-data
Required Service Data for Office	https://docs.microsoft.com/en-us/DeployOffice/privacy/required-service-data

IV.2.6. CMH-6 S'outiller pour mieux gérer son locataire (tenant) (pour grandes organisations)

Les grosses organisations ont fréquemment une administration décentralisée pour certaines fonctions en fonction des pays, des filiales…

La délégation des droits d'administration Office 365 à des équipes d'administration locale, selon des périmètres techniques ou selon l'organisation peut être simplifiée par des outils tiers. Ces outils tiers proposent de définir des organisations virtuelles et des rôles d'administration dédiés (et limités) à cette délégation.

Des outils tiers et des options soumises à licence permettent de faciliter l'automatisation de certaines tâches d'administration. Par exemple, des actions automatiques peuvent être déclenchées pour donner suite à une alerte. Des outils proposent des modèles de politiques de conformité ou de détection pour aider les grosses organisations à harmoniser la configuration du locataire (tenant) et par conséquent son niveau de sécurité.

La mise en place d'outils de gestion des identités et des accès permet de mieux contrôler les utilisateurs Office 365, en mettant en place des processus de revue des comptes.

De façon générale, il convient périodiquement de revoir l'usage des outils tiers avec les nouvelles fonctionnalités proposées par l'éditeur. Il est donc conseillé d'avoir une approche agile sans pour autant remettre systématiquement en cause les outils tiers. Cette revue doit prendre en compte les critères de coûts, de simplicité et de charges opérationnelles induites.

IV.2.7. CMH-7 Documenter la gestion du locataire (tenant)

Il est recommandé de créer une base de connaissances concernant le locataire (tenant) Office 365 de l'organisation. Cette documentation devra être maintenue dans le temps afin de tenir compte des évolutions côté Microsoft et des évolutions prévues côté organisation.

La base de connaissances doit comporter deux niveaux.

Tout d'abord, la documentation à destination d'équipes de production doit contenir :

- l'intégralité des informations liées à l'état du locataire (tenant) et le modèle d'administration :
  - rôles et responsabilités,
  - listes des administrateurs et droits associés ;
- la description des services et fonctionnalités choisis par l'organisation ;
- les traces des modifications réalisées ;

- les procédures et standards ;
  - procédures d'administration et de validation des changements,
  - procédures de support,
  - prérequis techniques,
  - standards de sécurité de la plateforme.

Ces informations doivent permettre de capitaliser les connaissances, permettre une continuité en cas de changements au sein de l'équipe d'administration et assurer une cohérence entre les différents services. Elles doivent également être source de référence dans des contextes d'organisation multientités.

Ensuite, il est nécessaire de maintenir à jour une base de connaissances à destination des utilisateurs, ou à défaut des relais pour l'adoption des services. Là encore, la documentation devra être tenue à jour en prenant en compte les évolutions régulières des différents services.

IV.2.8. CMH-8 Faciliter le travail en mode déconnecté

Pour limiter les impacts pour les utilisateurs en cas d'indisponibilité de l'accès aux services Office 365, il est recommandé d'installer sur les postes les versions Microsoft 365 Apps des applications. Le client OneDrive installé, les utilisateurs pourront continuer à travailler en mode déconnecté, la synchronisation s'effectuant automatiquement dès que le service sera de nouveau disponible. La fonction OneDrive de « fichiers à la demande » permettant d'économiser de l'espace disque devra être désactivée totalement ou uniquement sur les dossiers que l'on veut rendre obligatoirement disponibles hors connexion.

Guide de déploiement pour Microsoft 365 Apps	https://docs.microsoft.com/fr-fr/deployoffice/deployment-guide-microsoft-365-apps
Guide de déploiement pour Microsoft 365 Apps for Enterprise	https://docs.microsoft.com/fr-fr/DeployOffice/deployment-guide-for-office-365-proplus
Économisez de l'espace disque avec les fichiers à la demande OneDrive pour Windows 10	https://support.office.com/fr-fr/article/économisez-de-l-espace-disque-avec-les-fichiers-à-la-demande-onedrive-pour-windows-10-0e6860d3-d9f3-4971-b321-7092438fb38e

IV.2.9. CMH-9 Surveiller les performances des infrastructures d'accès et augmenter la bande passante si nécessaire

Le basculement sur l'utilisation de services cloud peut avoir des impacts importants sur les flux Internet entrants et sortants du réseau d'entreprise d'autant que certains usages comme la visioconférence ou le travail collaboratif offerts par les services Office 365 seront adoptés par les utilisateurs.

Pour minimiser ces impacts et s'assurer des meilleures performances (bande passante et temps de latence), Microsoft recommande d'implémenter des exceptions pour les flux Office 365 dans les systèmes de filtrage ou d'inspection réseau des sorties Internet (ces systèmes font double-emploi par rapport aux contrôles disponibles au niveau des services eux-mêmes). De plus, pour les sites distants, les flux Office 365 doivent être redirigés par le chemin le plus direct à travers les ISP vers les points d'accès les plus proches géographiquement plutôt que de « faire une boucle » en remontant par le site central pour

ressortir sur Internet. Enfin, dans le cadre du télétravail, il est recommandé, pour ne pas saturer le lien VPN et obtenir les meilleures performances de faire sortir uniquement les flux Office 365 sur Internet (Full VPN avec exceptions/Split tunneling), en faisant toujours transiter les autres flux dans le tunnel VPN.

Concernant plus particulièrement Teams, l'outil « tableau de bord de qualité des appels » permet de mesurer la qualité des appels et des réunions, au niveau de l'organisation.

Principes de connectivité réseau Microsoft 365	https://docs.microsoft.com/fr-fr/microsoft-365/enterprise/microsoft-365-network-connectivity-principles?view=o365-worldwide
URL et plages d'adresses IP Office 365	https://docs.microsoft.com/fr-fr/microsoft-365/enterprise/urls-and-ip-address-ranges?view=o365-worldwide
Implémentation d'un tunnel VPN partagé pour Office 365	https://docs.microsoft.com/fr-fr/microsoft-365/enterprise/microsoft-365-vpn-implement-split-tunnel?view=o365-worldwide
Qu'est-ce que le tableau de bord de qualité des appels ?	https://docs.microsoft.com/fr-fr/microsoftteams/cqd-what-is-call-quality-dashboard

IV.2.10. CMH-10 Mettre en œuvre des stations d'administration sécurisées et dédiées (PAW)

La mise en œuvre de postes d'administration (*Privileged Access Workstations,* ou PAW) a pour objectif de fournir aux administrateurs un environnement sécurisé dans lequel doivent s'exécuter des actions sensibles.

Ces environnements doivent notamment respecter les bonnes pratiques suivantes : pas de droits d'administration locale, contrôle des flux, restriction de la navigation Internet, contrôle des applications installées, mise en place de solution de type antivirus et EDR.

À noter, Microsoft fournit des guides pour l'implémentation de ces postes et de la restriction l'accès aux outils d'administration de la plateforme :

- **configurer un poste Windows10 spécifiquement pour les administrateurs ;**
- **utiliser un poste virtuel dans Azure sur la base d'un template proposé par Microsoft.**

Station de travail à accès privilégiés	https://docs.microsoft.com/fr-fr/windows-server/identity/securing-privileged-access/privileged-access-workstations
Station virtuelle d'administration dans Azure	https://docs.microsoft.com/en-us/azure/active-directory/devices/howto-azure-managed-workstation
Administration sécurisée des systèmes d'information	https://www.ssi.gouv.fr/uploads/2015/02/guide_admin_securisee_si_anssi_pa_022_v2.pdf
L'administration en silo	https://www.sstic.org/media/SSTIC2017/SSTIC-actes/administration_en_silo/SSTIC2017-Article-administration_en_silo-bordes.pdf
Guide ANSSI, *Mise en œuvre des fonctionnalités de sécurité de Windows 10 reposant sur la virtualisation*	https://www.ssi.gouv.fr/guide/mise-en-oeuvre-des-fonctionnalites-de-securite-de-windows-10-reposant-sur-la-virtualisation/

Les administrateurs ne peuvent utiliser leur compte d'administration que sur les postes PAW (*via* le mécanisme de silo d'authentification AD) après une authentification forte.

IV.2.11. CMH-11 Déterminer l'indisponibilité effective du service Office 365

Ce qui peut être pris comme une indisponibilité du service Office 365 peut être lié à d'autres éléments comme des problèmes réseau ou un service interne de fédération d'identités. Il est donc nécessaire de vérifier en premier lieu la disponibilité du service Office 365 qui peut être contrôlée en temps réel par le portail d'administration Office 365. L'état de santé de l'ensemble des services est indiqué et les avis détaillant les éventuels problèmes constatés et leur statut de même qu'un historique.

Vérifier l'état du service Office 365	https://docs.microsoft.com/fr-fr/office365/enterprise/view-service-health

Si le service est indiqué comme disponible, il peut s'agir d'un problème d'inaccessibilité lié au réseau ou de l'indisponibilité d'un autre composant de la chaîne. Par exemple, lorsque l'organisation s'appuie sur la fédération d'identités pour implémenter le SSO entre son annuaire Active Directory interne et Azure AD (qui gère l'authentification pour l'accès aux services Office 365), la disponibilité des serveurs de fédération déployés en interne doit être vérifiée. Si le service de fédération interne n'est pas disponible, l'accès aux services Office 365 sera impossible alors que ces derniers sont accessibles et disponibles.

IV.3. Mesures de gestion des identités et des accès à Office 365

IV.3.1. CMI–1 Mettre en place une authentification renforcée

Cette mesure consiste à activer **l'authentification multifacteur (MFA)**. Après enregistrement de son mobile, l'utilisateur devra fournir, en plus de son mot de passe, un second facteur comme preuve de possession (appel téléphonique, application d'authentification Microsoft Authenticator). L'authentification MFA est disponible de base pour l'ensemble des utilisateurs d'Office 365.

L'authentification multifacteur n'est pas activée par défaut pour les comptes d'administrateur globaux. Il est très fortement recommandé d'activer dès le début du déploiement cette fonctionnalité pour protéger ces comptes à pouvoir.

Des solutions tierces de MFA peuvent être déployées à condition de mettre en place de la fédération d'identités.

Pour contrer les attaques de phishing les plus évoluées, une mesure efficace est l'utilisation d'authentificateurs compatibles avec le **standard FIDO2.** Ce type de technologie permet de se prémunir, par conception, contre le phishing. En effet, FIDO2 n'utilise pas de mot de passe et vérifie l'URL du fournisseur d'identité avant de dérouler l'authentification et la signature d'un challenge à l'aide d'une clé privée stockée localement sur l'authentificateur après vérification de l'identité de l'utilisateur.

Comment obtenir Azure Multi-Factor Authentication ?	https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/concept-mfa-licensing
Protéger vos comptes d'administrateur général Office 365	https://docs.microsoft.com/fr-fr/office365/enterprise/protect-your-global-administrator-accounts

Configurer l'authentification multifacteur	https://docs.microsoft.com/fr-fr/office365/admin/security-and-compliance/set-up-multi-factor-authentication?view=o365-worldwide
Recommandations de stratégie de mot de passe pour Office 365	https://docs.microsoft.com/fr-fr/office365/admin/misc/password-policy-recommendations?view=o365-worldwide

À défaut, il faut mettre en place une politique de mot de passe adaptée.

Cette mesure consiste à mettre en place une politique de mots de passe en suivant les bonnes pratiques actuelles. Ces dernières peuvent sembler contre-intuitives, mais correspondent aux menaces actuelles ; ne pas forcer un renouvellement des mots de passe hors suspicion de compromission, ne plus exiger des mots de passe longs ou complexes, mais, par contre, bannir l'utilisation de mots de passe communs.

Des actions de sensibilisation auprès des utilisateurs sont également nécessaires pour leur rappeler ces bonnes pratiques, comme le fait de ne pas utiliser les authentifiants de l'organisation pour se connecter à des sites Web externes.

Azure AD Password Protection détecte et bloque les mots de passe faibles connus et leurs variantes, le dictionnaire étant dynamiquement enrichi de l'analyse et de la télémétrie de sécurité Azure AD.

Éliminer les mots de passe incorrects de votre organisation	https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/concept-password-ban-bad
Présentation d'Azure Active Directory Password Protection	https://docs.microsoft.com/fr-fr/azure/active-directory/authentication/concept-password-ban-bad

Il faut également forcer les réauthentifications par les cookies et jetons d'accès.

L'option « Rester connecté » qui est proposée à l'utilisateur lors d'une connexion à Office 365 a été ajoutée pour limiter le nombre de fois où l'utilisateur doit se réauthentifier, en créant un cookie persistant après fermeture du navigateur. Face à ce constat, une mesure consiste à ne pas proposer cette option en désactivant la politique Azure AD « Afficher l'option permettant de rester connecté ».

Il est également possible de jouer plus précisément sur les durées des différents jetons (accès, actualisation et session) par le biais de politiques d'accès conditionnel.

Les politiques d'accès conditionnel prévalent sur l'option « Rester connecté ». Cela veut dire qu'un utilisateur soumis à une politique d'accès conditionnel forçant les jetons non persistants ne pourra pas bénéficier de la fonctionnalité.

Il convient de noter également que les politiques d'accès conditionnel sont désormais évaluées en continu, ce qui permet par exemple de forcer une réauthentification en cas de changement de réseau.

Personnaliser la page de connexion Azure Active Directory de votre organisation (Fonctionnalité : « Resté connecté » ou « *Keep me signed* »)	https://docs.microsoft.com/fr-fr/azure/active-directory/fundamentals/customize-branding
Configurer la gestion de session d'authentification avec l'accès conditionnel	https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/howto-conditional-access-session-lifetime

IV.3.2. CMI–2 Mettre en place une gestion des arrivées/départs

Cette mesure est importante pour la sécurité de l'organisation au-delà d'Office 365. Les comptes permettant l'accès à Office 365 doivent être créés dans le processus d'arrivée et ils doivent être désactivés, puis supprimés dans le processus de départ.

Ces processus peuvent être manuels – sous la responsabilité d'une entité de l'organisation, mais à partir d'une certaine taille de l'organisation, il est vivement conseillé d'automatiser ces processus en lien lorsque c'est possible avec une solution de gestion des identités et des accès (Solution IAM). Cette automatisation permet de fluidifier le processus de création de comptes dans Azure AD, de mettre en place des contrôles et de rendre systématiques les désactivations de comptes lors du départ de l'utilisateur.

Pour renforcer ces processus, il est conseillé de mettre en place une ou plusieurs étapes d'approbation, notamment pour les comptes administrateurs Office 365 – ayant un ou plusieurs rôles d'administration de la solution. Cette étape d'approbation peut avoir aussi un rôle de modération lorsqu'une création a un impact sur les coûts de licences.

Il est important que le processus de gestion des départs intègre une notification systématique des managers afin de les sensibiliser au besoin de statuer sur les changements de propriétaire nécessaire (par exemple l'utilisateur quittant l'organisation est le propriétaire unique d'un SharePoint Online : son manager doit définir si ce SharePoint doit être archivé ou bien s'il doit changer de propriétaire pour assurer la pérennité de la gestion du contenu du SharePoint).

IV.3.3. CMI–3 Mettre en place une revue des comptes et privilèges

Afin de garantir une bonne hygiène de l'administration et suivre le principe de moindre privilège, il est indispensable de revoir régulièrement les utilisateurs ayant des rôles d'administration et lesdits rôles. Tout rôle doit être justifié et donné pour une durée limitée.

Une revue régulière (tous les 3 mois minimum) doit permettre de contrôler qu'un utilisateur n'ait pas de rôles trop élevés à la suite d'une modification de son périmètre ou de prolonger les droits si nécessaire.

La revue de comptes à privilèges peut se faire :

- **manuellement** ;
- **automatiquement** *via* les mécanismes de revues des accès inclus dans Azure Privileged Identity Management.

Dans tous les cas, une justification doit être obtenue et validée par les instances de gouvernance de la plateforme.

À noter, certains outils d'IAM tierces permettent de provisionner des comptes d'administration et proposent également des fonctionnalités de revue.

IV.3.4. CMI–4 Assurer la disponibilité de l'authentification

Plusieurs scénarios d'authentification existent avec Office 365. Les scénarios Pass-through Authentication et d'identité fédérées imposent la disponibilité des infrastructures internes.

Pour le scénario PTA, il faut installer au minimum trois agents d'authentification PTA.

Pour assurer la disponibilité d'un service de fédération interne qui conditionnera la disponibilité de l'accès à l'authentification d'Office 365, il est important de réfléchir à ces bonnes pratiques :

- le service de fédération interne doit être correctement dimensionné pour supporter les pics d'authentification en fonction du nombre d'utilisateurs ;

- le service de fédération doit être disponible en déployant plusieurs serveurs de fédération pour faire face à la panne d'un serveur de fédération ;
- si le service AD FS *(Active Directory Federation Service)* est utilisé, mettre en place le verrouillage intelligent extranet (ESL) pour protéger contre le verrouillage de comptes extranet lié à des activités malveillantes ;
- mettre en place un système de surveillance de la disponibilité du service de fédération par exemple Azure AD Connect Health ou autre.

Plus d'informations

AD FS le verrouillage extranet et le verrouillage intelligent extranet	https://docs.microsoft.com/fr-fr/windows-server/identity/ad-fs/operations/configure-ad-fs-extranet-smart-lockout-protection
Pourquoi utiliser Azure AD Connect Health ?	https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/whatis-azure-ad-connect#why-use-azure-ad-connect-health
Scénario Pass-through Authentication	https://docs.microsoft.com/fr-fr/azure/active-directory/hybrid/how-to-connect-pta-quick-start#step-4-ensure-high-availability

IV.3.5. CMI–5 Maîtriser les appareils autorisés à accéder à Office 365

La première mesure consiste à former les utilisateurs pour qu'ils mettent systématiquement un mot de passe ou code PIN pour protéger leurs propres données et l'accès à leurs applications professionnelles, comme Office 365, ou personnelles (réseaux sociaux, banque…). L'application de cette mesure peut être contrôlée sur les appareils fournis par l'organisation et il convient de mettre en place des mesures organisationnelles ou techniques pour maîtriser les appareils.

L'outil privilégié pour la gestion des appareils de l'organisation est le MDM (Mobile Device Management) qui permet de gérer aussi bien des appareils mobiles, smartphones, tablettes (iOS et Android) que des postes de travail (Windows, macOS, Linux).

Une fois enregistré dans le MDM, l'appareil va pouvoir être géré d'un point de vue sécurité : on lui affectera des stratégies de sécurité pour imposer par exemple un code PIN avec un niveau de complexité, un niveau minimum de version d'OS, le chiffrement du stockage, le fait que l'appareil n'ait pas été compromis ou déplombé *(jailbroken),* etc.

Si, à un instant donné, l'appareil ne devait plus respecter la politique de sécurité imposée, il serait considéré comme non conforme et se verrait refuser l'accès à certaines ressources de l'organisation ou, *a minima,* n'avoir que des accès restreints. Ce contrôle doit s'effectuer non seulement pour les accès Web, mais aussi pour l'accès à travers les applications, qu'il s'agisse des applications Office installées sur un poste Windows ou des applications Office Mobile disponibles sur les autres plateformes (iOS, Android).

La fonction MDM d'Office 365 (disponible de base) s'applique aux appareils mobiles et permet d'imposer que l'appareil soit enregistré et qu'il respecte les politiques de sécurité sans quoi l'accès à Office 365 *via* les applications mobiles sera bloqué. Pour la prise en charge des PC Windows 10, il est nécessaire d'utiliser Microsoft Intune ou un autre MDM).

Fonctionnalités de gestion des appareils mobiles intégrées à Office 365	https://support.office.com/fr-fr/article/fonctionnalités-de-gestion-des-appareils-mobiles-intégrées-à-office-365-a1da44e5-7475-4992-be91-9ccec25905b0

Contrôler l'accès depuis des appareils non enregistrés	https://docs.microsoft.com/fr-fr/sharepoint/control-access-from-unmanaged-devices

IV.3.6. CMI–6 Mettre en place un processus de gestion des services tiers

La mesure consiste à limiter l'accès au store et les possibilités d'installation d'applications tierces non validées.

Pour éviter que les utilisateurs finaux ne soient autorisés à connecter des applications/services tiers, il est nécessaire de mettre en place le « consentement administrateur ».

Cette option consiste à faire valider par un (ou plusieurs) administrateur(s) les droits que nécessite l'application d'entreprise désirée avant qu'elle soit connectée à l'environnement Office 365.

Attention, il faut bien garder à l'esprit que cette option bloque l'utilisation de nouvelles applications connectées à Office 365 tant que celles-ci n'ont pas été validées.

Explication du consentement administrateur	https://docs.microsoft.com/en-us/microsoft-365/admin/misc/integrated-apps
Configuration du workflow de consentement d'administrateur	https://docs.microsoft.com/en-us/azure/active-directory/manage-apps/configure-admin-consent-workflow

La gestion de l'accès au « Microsoft Store » permet aussi de sécuriser votre environnement en évitant l'installation d'applications tierces potentiellement dangereuses.

L'idée ici est de mettre en place un store d'entreprise dans lequel vous pourrez gérer les applications disponibles ainsi que les options de mise à disposition.

Mise en place d'un « Store Microsoft pour Entreprises »	https://docs.microsoft.com/fr-fr/microsoft-store/

IV.3.7. CMI–7 Implémenter un cycle de vie des utilisateurs invités

Dans le cadre de la gouvernance des accès « invité », le cycle de vie d'un utilisateur externe invité doit être maîtrisé : création/utilisation et suppression.

La création d'un utilisateur invité se fait en deux étapes : l'ajout dans l'annuaire Azure Active Directory et l'attribution de droits sur les ressources.

Par défaut, un utilisateur externe peut être invité par l'intermédiaire des interfaces d'administration (Azure AD par exemple), lors de l'envoi d'un lien de partage ou encore lors de l'ajout à un Groupe Microsoft 365.

Les paramétrages d'Office 365 permettent de déterminer si l'invitation d'utilisateur externe peut être réalisée directement par les utilisateurs internes ou si elle doit suivre un processus spécifique :

- ajout *via* un portail dédié ou intégré dans l'ITSM de l'organisation ;
- validation hiérarchique ou par une équipe dédiée ;
- conservation des informations liées à l'invitation (ces informations sont présentes au sein du journal d'activité Office 365 qui dispose d'une profondeur de log de 90 à 365 jours en

fonction de la licence Office 365 détenue, il est donc pertinent d'exporter ces informations régulièrement).

Une fois l'utilisateur invité, il est nécessaire de s'assurer qu'il respecte les politiques de sécurité de l'organisation. En effet, l'organisation source est responsable de l'identification et de l'authentification de l'invité, mais l'organisation accueillante est responsable de la gestion des accès et de la protection des données.

L'idéal est d'utiliser des stratégies d'accès conditionnel (*via* les options Microsoft ou un service tiers) pour s'assurer qu'un utilisateur externe soit soumis à de l'authentification multifacteur, signe une charte de bonnes pratiques, ne puisse accéder qu'en mode Web, ne pas synchroniser de librairies de document avec son poste personnel, etc.

Concernant la suppression, Microsoft ne propose rien par défaut pour s'assurer que les utilisateurs soient bien supprimés. Un processus doit être défini pour revoir les invités manuellement ou automatiquement selon des conditions (après une durée prédéfinie, après une durée d'inactivité prédéfinie, sur demande des utilisateurs internes, etc.).

Pour plus d'informations :

Informations de référence sur les paramètres de partage d'invités de Microsoft 365	https://docs.microsoft.com/en-us/microsoft-365/solutions/microsoft-365-guest-settings?view=o365-worldwide

IV.4. Mesures de protection de l'information stockée dans Office 365

IV.4.1. CMP-1 Classifier les documents et messages

Cette mesure traite de la classification des documents et des messages, et par conséquent indirectement des données qu'ils contiennent. Cette classification est basée sur un système d'étiquetage soit assisté par une solution soit mise en place par des conventions de nommage pour les documents ou des conventions applicables aux objets des messages.

La classification doit être simple pour être applicable par tous les utilisateurs. Elle permet une représentation des niveaux de sensibilité, mais également des champs d'application d'un message ou d'un document.

Chaque organisation doit définir une classification des documents ou des messages contenus dans Office 365 qui lui est propre en fonction de ses impératifs et règles métiers ou ses impératifs réglementaires.

Les documents ou les messages pouvant contenir des données de sensibilités différentes, la règle de classification doit préciser si c'est le plus haut degré de sensibilité qui s'applique en fonction de la politique de sécurité des données définie par l'organisation.

Par exemple dans le domaine métier des ressources humaines peuvent coexister des documents avec divers degrés de classification :

- **public : une offre d'emploi publiée sur un site Web ;**
- **restreint à l'organisation : l'organigramme de la société ;**
- **confidentiel : les données salariales ou les données réglementées (RGPD, avec des contraintes supplémentaires pour les données de santé) ;**
- **strictement confidentiel : La stratégie RH d'évolution de la courbe des âges.**

L'entreprise doit être en conformité avec les réglementations et définir ses règles d'usage d'Office 365 pour des données auxquelles s'appliquent des contraintes particulières.

IV.4.2. CMP-2 Protéger les informations sensibles par chiffrement

Avant de mettre en place des solutions de chiffrement supplémentaires, il convient de savoir quelles sont les solutions de chiffrement utilisées de base sur les services Office 365.

Chiffrement au repos au niveau service

Les services Exchange Online, SharePoint Online, OneDrive for Business, Teams et Yammer bénéficient du chiffrement de leurs données au repos. Cette fonctionnalité est implémentée au niveau du service lui-même et est référencée dans la documentation Microsoft comme « chiffrement au niveau service » (Service Encryption). L'implémentation peut être différente selon le service : par exemple, Exchange Online implémente le chiffrement au niveau de la boîte aux lettres, alors que SharePoint Online et OneDrive for Business offre un chiffrement au niveau fichier. Ce chiffrement vient en complément du chiffrement BitLocker au niveau des disques des serveurs des centres de données.

Par défaut, le chiffrement au niveau service utilise des clés de chiffrement maître ou racine (root key) créées et gérées par le service lui-même.

Chiffrement au repos avec clé client (et option Bring Your Own Key ou BYOK)

Le client a la possibilité d'imposer ses propres clés racines, générées dans un Azure Key Vault en s'appuyant sur un HSM hébergé dans un centre de données Microsoft, ou en les transférant depuis un HSM local au client dans le HSM du centre de données. Cette dernière option est référencée dans la littérature Microsoft comme chiffrement au niveau service avec clé client (Service encryption with Customer Key).

Concernant plus particulièrement le support du chiffrement avec clé client sont couverts : le contenu des sites SharePoint Online et les fichiers stockés sur ces sites et les fichiers téléchargés sur OneDrive for Business et Teams ; le contenu des boîtes aux lettres Exchange Online (corps de message, entrées d'agenda et contenu des pièces jointes).

L'objectif principal est d'aider les clients à **respecter les obligations réglementaires** ou de conformité pour le contrôle des clés racines.

Pour plus d'informations :

Service Encryption with Customer Key For Office 365 FAQ	https://docs.microsoft.com/fr-fr/microsoft-365/compliance/customer-key-overview?view=o365-worldwide

Classification et chiffrement avec Azure Information Protection

Pour protéger les données sensibles, il faut être déjà en mesure de les identifier, les classifier pour ensuite les protéger en fonction de leur sensibilité.

Azure Information Protection (AIP) est une solution intégrée à Office 365 qui permet de classifier et, facultativement, de protéger les documents et messages en y appliquant des étiquettes. Les étiquettes peuvent être appliquées :

- automatiquement à travers des règles et des conditions définies par les administrateurs,
- ou manuellement par les utilisateurs, qui peuvent éventuellement recevoir des suggestions.

Les données sensibles peuvent être automatiquement chiffrées avec le service Azure Rights Management (Azure RMS), ce chiffrement apportant une protection même lorsque les fichiers sortent de l'entreprise.

Liens utiles

Qu'est-ce qu'Azure Information Protection ?	https://docs.microsoft.com/fr-fr/azure/information-protection/what-is-information-protection

Chiffrement avec une totale indépendance de Microsoft

Dans ce cas les clés doivent être stockées dans un HSM physique ; non seulement les clés ne sont pas accessibles par Microsoft, mais les données sont aussi indéchiffrables par les services Office 365. Ce qui assure un niveau de confidentialité maximal avec comme contrepartie des restrictions sur certaines fonctionnalités.

Deux types de solutions techniques sont déployables :

- **utilisation d'un système de Type Hold your own key (HYOK) en conjonction avec AIP, remplacé par Double Key Encryption (DKE).** Dans cette option, les données sont alors indéchiffrables par les services Office 365. Cette option consiste à chiffrer les fichiers au préalable avant de les déposer dans des espaces de stockage Office 365 ou de les attacher à des messages avec des clés dont vous maîtrisez la génération et la distribution pour assurer que les destinataires soient en mesure de les déchiffrer. Ces solutions ont l'avantage de rendre totalement opaques les données vis-à-vis des services Office 365 qui sont alors utilisés comme simples moyens de stockage ou de transport. Par contre, cela se fait au détriment de fonctionnalités : vous perdez les fonctions de collaboration, eDiscovery dans le cadre d'actions légales, de détection anti-malware mais aussi d'indexation et les métadonnées ;
- **chiffrement avec solution tierce**. Les mécanismes sont les mêmes que ci-dessus. Cela se fait au détriment de fonctionnalités : vous perdez les fonctions de collaboration, eDiscovery dans le cadre d'actions légales, de détection anti-malware, Vous conserver les fonctions d'indexation, de recherche de documents même si ce ne sont pas celles natives de Microsoft. Les métadonnées sont aussi conservées permettant une exécution des workflows.

IV.4.3. CMP-3 Limiter les droits d'accès aux documents partagés en externe

Le partage de documents avec des utilisateurs externes est une fonctionnalité importante dès lors que l'on travaille avec des partenaires. Plutôt que de laisser les utilisateurs user de moyens détournés, il vaut mieux leur offrir des possibilités de partager des documents ou des dossiers tout en gardant le contrôle.

Cependant, pour assurer un partage d'information de manière sécurisée, il est important d'appliquer un certain nombre de bonnes pratiques parmi lesquelles :

- définir et appliquer une politique de partage au niveau de l'organisation qui doit s'appliquer aux solutions de partage SharePoint, OneDrive, Teams et les Groupes Microsoft 365. Il est possible d'imposer des restrictions de partage au niveau global de l'organisation ;
- interdire le partage pour utilisateurs non authentifiés : ceci permet d'imposer que tous les utilisateurs externes soient visibles dans l'annuaire, d'auditer les accès et contrôler leurs permissions ;
- imposer une authentification multifacteur pour les comptes « invité » : étant donné que les utilisateurs invités peuvent utiliser des comptes de messagerie personnels qui ne sont

soumis à aucune stratégie de gouvernance, il est particulièrement intéressant d'exiger une authentification multifacteur pour les invités ;

- isoler les données sensibles et les héberger sur des sites sur lesquels vous n'autoriserez pas le partage externe ;
- former les utilisateurs sur l'utilisation des partages vers l'extérieur que ce soit à partir de SharePoint, OneDrive ou Teams, et à respecter des bonnes pratiques comme partager au niveau document plutôt que site, et assurer le contrôle des sites ou canaux dont ils sont responsables ;
- appliquer le principe du moindre privilège avec les permissions Office 365 comme cela devait être le cas pour les solutions internes ; par exemple la définition d'un responsable de site SharePoint à qui revient la responsabilité des autorisations d'accès ;
- auditer régulièrement les partages externes à travers le portail d'administration, les fonctionnalités d'audit d'Office 365 (soumis à niveau de licence) ou à l'aide de solutions tierces pour s'assurer du respect de la politique de sécurité.

Liens utiles :

Collaborer avec des invités sur un document	https://docs.microsoft.com/fr-fr/microsoft-365/solutions/collaborate-on-documents?view=o365-worldwide#sharepoint-organization-level-default-link-settings
Configurer le stockage et le partage des fichiers	https://docs.microsoft.com/fr-fr/microsoft-365/admin/setup/set-up-file-storage-and-sharing?view=o365-worldwide
Créer un environnement de partage d'invités sécurisé	https://docs.microsoft.com/fr-fr/microsoft-365/solutions/create-secure-guest-sharing-environment?view=o365-worldwide
Gérer l'accès « invité » dans les groupes Microsoft 365	https://docs.microsoft.com/fr-fr/microsoft-365/admin/create-groups/manage-guest-access-in-groups?view=o365-worldwide
Gérer l'accès « invité » dans Microsoft Teams	https://docs.microsoft.com/fr-fr/microsoftteams/manage-guests
Vue d'ensemble du partage externe	https://docs.microsoft.com/fr-fr/sharepoint/external-sharing-overview

IV.4.4. CMP-4 Définir un processus de récupération des données

L'organisation doit mettre en place un processus de récupération des fichiers ou éléments de messagerie afin d'être en mesure de restaurer :

- du contenu supprimé par erreur ou supprimé à la suite du dépassement du délai de rétention ;
- du contenu appartenant à des utilisateurs ayant quitté l'organisation ;
- pour répondre à une demande réglementaire.

Le processus doit préciser les règles de validation des demandes de restauration.

La restauration par les mécanismes Microsoft est possible lorsque la durée de rétention est inférieure à l'âge du contenu à restaurer. Selon le type de licence détenue, la période de rétention est plus ou moins longue.

Il est possible de mettre en place une politique d'archivage pour conserver certains contenus, mais ces outils ne prennent pas en compte les éléments supprimés.

Au-delà de cette durée de rétention, il est nécessaire de mettre en place des outils de sauvegarde tiers. Ces outils permettent une maîtrise des données de l'organisation en mettant en œuvre une duplication totale ou partielle des contenus, une indexation des contenus sauvegardés et une capacité de restauration indépendante du contrat avec Microsoft. Les données peuvent être sauvegardées dans le cloud ou dans les datacenters de l'organisation.

Un mécanisme spécifique à la messagerie permet de désigner une boîte aux lettres « en conservation pour litige ». Dans ce cas, tous les contenus originaux sont conservés, quelles que soient les actions de son propriétaire.

Placement d'une boîte aux lettres en conservation pour litige	https://docs.microsoft.com/fr-fr/exchange/policy-and-compliance/holds/litigation-holds?view=exchserver-2019

IV.4.5. CMP-5 Gérer les applications avec un outil de gestion des applications mobiles

Pour le cas des appareils mobiles personnels, une solution moins contraignante que d'imposer le contrôle par un MDM, consiste à contrôler les applications par un outil de gestion MAM (Mobile Application Management). Cet outil permet de choisir quelles applications seront déployées sur quels appareils mobiles avec un ciblage par catégories ou groupes d'utilisateurs **sans imposer que le mobile soit enregistré dans le MDM**. Il est possible de configurer les paramètres spécifiques à chaque application comme la langue, la sécurité, ou une personnalisation de l'organisation.

Dans le cas d'Office 365, les applications Office Apps (Outlook, Excel, Word, OneNote, OneDrive…) sont intégrées avec la fonctionnalité MAM du MDM Microsoft Intune.

Qu'est-ce que la gestion des applications Microsoft Intune ?	https://docs.microsoft.com/fr-fr/intune/apps/app-management

IV.4.6. CMP-6 Mettre en place le contrôle d'accès conditionnel

L'objectif de cette mesure est de définir les conditions applicables à l'utilisateur, à son appareil et à son accès pour autoriser un usage d'Office 365. Par exemple, cela permet d'interdire une connexion depuis un appareil BYOD non équipé d'antivirus.

La mesure consiste à limiter ou autoriser l'accès à Office 365 sous certaines conditions. Cette fonctionnalité de **contrôle d'accès conditionnel** est implémentée par Azure AD et permet d'appliquer des stratégies de sécurité qui sont déclenchées automatiquement lorsque certaines conditions sont remplies. Il est par exemple possible de bloquer l'accès si les données de contexte suggèrent que l'utilisateur a été compromis ou s'il est très improbable que l'utilisateur se connecte dans ces conditions ; on peut refuser la connexion depuis un poste non enregistré et dont l'état de santé n'est pas connu ou lui donner un accès uniquement en lecture seule à sa boîte aux lettres sans possibilité de télécharger localement les pièces jointes, etc.

Les conditions peuvent se baser sur l'appartenance à des groupes d'utilisateurs, l'emplacement depuis lequel s'effectue la connexion, le risque calculé, le type d'appareil, son état de santé et l'application. Lorsqu'une condition est remplie, la stratégie Azure AD pourra :

- exiger l'authentification multifacteur pour prouver l'identité ;

- modifier les actions que l'utilisateur peut prendre dans les applications cloud ;
- restreindre l'accès aux données sensibles, par exemple, limiter les téléchargements ou les fonctionnalités de partage ;
- exiger la réinitialisation du mot de passe ;
- bloquer l'accès.

En environnement Office 365, il est possible de **paramétrer SharePoint Online et OneDrive pour limiter les droits de l'utilisateur lorsqu'il accède depuis un poste non conforme**. Un bandeau jaune s'affiche en haut du navigateur pour indiquer à l'utilisateur qu'il ne pourra pas télécharger, imprimer ou synchroniser localement les documents auxquels il accède. Cette protection permet de lutter contre les fuites d'information même involontaires tout en laissant la possibilité à l'utilisateur d'accéder à ses documents et de les modifier sachant qu'ils ne pourront pas quitter le stockage sécurisé de l'organisation.

Exchange Online offre le même type de restrictions lorsque l'utilisateur accède à sa messagerie à partir d'un poste non conforme. Il pourra lire ses courriers, accéder en lecture aux documents attachés ou les sauvegarder sur son OneDrive for Business, mais sans pouvoir les copier localement.

Pour plus d'informations, consultez les articles ci-dessous :

Qu'est-ce que l'accès conditionnel ?	https://docs.microsoft.com/fr-fr/azure/active-directory/conditional-access/overview
Stratégies communes pour les identités et l'accès aux appareils	https://docs.microsoft.com/fr-fr/microsoft-365/enterprise/identity-access-policies
Tarification Azure Active Directory	https://azure.microsoft.com/fr-fr/pricing/details/active-directory/
Contrôler l'accès (SharePoint et OneDrive) depuis des appareils enregistrés	https://docs.microsoft.com/fr-fr/sharepoint/control-access-from-unmanaged-devices
Conditional Access in Outlook on the web for Exchange Online	https://techcommunity.microsoft.com/t5/Outlook-Blog/Conditional-Access-in-Outlook-on-the-web-for-Exchange-Online/ba-p/267069

IV.4.7. CMP-7 Interdire la synchronisation des données depuis les appareils non gérés

Cette mesure technique a pour objectif d'interdire la synchronisation des données en provenance des services Exchange Online et OneDrive For Business depuis des appareils non gérés par l'organisation. Ceci permet de limiter les risques de fuite d'information si les données sont copiées sur des matériels non protégés (par exemple PC personnel sans chiffrement disque) et qui ne respecte pas les politiques de sécurité de l'organisation.

Il est possible simplement d'autoriser la synchronisation OneDrive uniquement sur des appareils joints à des domaines spécifiques.

Cette mesure est liée à CMH-2 Durcissement des configurations des services de collaboration.

Tutoriel pour protéger sa messagerie des appareils non managés	https://docs.microsoft.com/fr-fr/mem/intune/protect/tutorial-protect-email-on-unmanaged-devices

Restriction de synchronisation OneDrive	https://docs.microsoft.com/fr-fr/onedrive/allow-syncing-only-on-specific-domains

IV.4.8. CMP-8 Respecter les bonnes pratiques liées à l'utilisation de Customer Key

Une analyse de risques doit être réalisée pour définir la façon dont seront protégées les données. Le chiffrement des données au repos peut s'appuyer sur différents mécanismes.

Les différents services de chiffrement Office 365 utilisent Azure Key Vault (stockées directement dans Azure ou dans un HSM).

Compte tenu des impacts potentiels importants pouvant entraîner des interruptions de service ou une perte irrévocable de vos données, il est nécessaire de suivre les recommandations pour la mise en œuvre et l'administration telles que détaillées dans l'article **Configurer la clé client**.

Parmi ces recommandations, la création de 2 souscriptions Azure dédiées pour la mise en œuvre de Customer Key et de 2 Key Vaults dédiés par service (par exemple une paire pour Exchange Online et une autre paire pour SharePoint Online). D'un point de vue administration, il est recommandé de séparer les administrateurs selon les services.

Concernant, les procédures de récupération, activer la fonctionnalité de suppression récupérable, sauvegarder les coffres de clés sur des supports hors-ligne une fois les clés transférées, et s'assurer que la procédure de récupération utilisant la clé de disponibilité (en cas de vol du contrôle des coffres-forts) est en place.

Configurer la clé client	https://docs.microsoft.com/fr-fr/microsoft-365/compliance/customer-key-set-up?view=o365-worldwide
En savoir plus sur la disponibilité de la clé client	https://docs.microsoft.com/fr-fr/microsoft-365/compliance/customer-key-availability-key-understand?view=o365-worldwide#availability-key-uses

Il est possible de mettre en place des mécanismes complémentaires pour gérer les clés dans un HSM et maîtriser la création des clés dans une PKI appartenant à l'organisation. Ces solutions permettent de réduire le risque de divulgation des données au fournisseur ou aux autorités auxquelles il est assujetti.

IV.5. Mesures de détection des événements sécurité Office 365

Ce chapitre traite des mesures basées sur la collecte, le stockage et l'exploitation des logs, des objets techniques de configuration et des metadata mis à disposition par les systèmes opérants. Nativement, les fonctionnalités d'audit d'Office 365 proposent une expérience d'audit unifiée regroupant l'ensemble des activités des utilisateurs et administrateurs sein d'un abonnement Office 365.

Les logs Office 365 accessibles à travers les Unified Audit Logs sont inaltérables – c'est-à-dire non modifiables ni supprimables par les administrateurs de l'entreprise. Ces logs sont accessibles et exportables *via* les centres de conformité et de sécurité, les API Office 365 Management et PowerShell. Il est possible de configurer directement des alertes liées à l'occurrence de certains logs dans les centres de sécurité et de conformité.

Lorsque la recherche dans le journal d'audit est activée, l'activité des utilisateurs et des administrateurs est enregistrée dans le journal d'audit et conservée au minimum pendant 90 jours.

L'exploitation des logs Office 365 peut se faire :

- *via* le portail sécurité du locataire (tenant) ;
- *via* une redirection des logs vers une infrastructure de traitement de logs ;
- *via* des services managés, mettant en œuvre leur propre service de traitement de logs.

Le délai de rétention des logs doit être adapté aux besoins de l'organisation comme le reste des données. Une attention particulière doit être faite sur la volumétrie des logs, en particulier si l'organisation décide de les exporter en dehors du locataire (tenant).

IV.5.1. CMD-1 Monitorer les modifications de configuration

Le premier niveau de surveillance concerne les modifications apportées par les administrateurs sur la configuration du locataire (tenant). Pour cela il est conseillé de :

- tracer l'ensemble des opérations d'administration sur le locataire (tenant) ;
- détecter les changements dans cette configuration qui participent à la diminution du niveau de sécurité du locataire (tenant) ;
- détecter les changements de configuration d'une ressource Office 365 par un administrateur (délégation, partage, ajout d'un membre dans un groupe, modération dans une liste de distribution) ;
- détecter les nouvelles règles de transfert messagerie *(transport rules, journal rules)* et les *send connectors* ;
- détecter l'altération ou l'arrêt de la génération des logs des comptes d'administration.

Selon les besoins de l'organisation, il est également conseillé de surveiller certains paramétrages pour les utilisateurs sensibles, en particulier :

- détecter les changements de la configuration messagerie de l'utilisateur (par exemple, les règles de transfert *inbox rules*) ;
- détecter l'altération ou l'arrêt de la génération des logs des comptes utilisateur (bypass, diminution de la rétention des logs, diminution de la période de conservation).

Si l'organisation est équipée d'une solution de détection, celle-ci permet en général de collecter toutes les opérations réalisées par les administrateurs *via* leur compte à privilège. Lorsque l'opération (la commande exécutée) peut conduire à une fuite d'information, elle doit être en mesure de l'identifier en quasi-temps réel et d'alerter les équipes de sécurité.

IV.5.2. CMD-2 Monitorer les usages

Le deuxième niveau de surveillance concerne l'usage d'Office 365 par les utilisateurs, en particulier les scénarios d'usage jugés contraires à la sécurité de l'organisation.

Il convient donc de définir les scénarios d'usage qui doivent être surveillés et qui déclencheront une alerte.

La liste ci-dessous présente des exemples que chaque organisation doit contextualiser :

- contexte de connexion à Office 365 interdit (incluant moyen habituel de connexion, appareils utilisés…) ;
- tentative de délégations illégitimes, de partages illégitimes, de lancement d'applications illégitimes ;

- usage de protocoles sensibles (POP, IMAP, Powershell …) ou de protocoles généralement non utilisés par les utilisateurs ;
- tentative de brute force pour anticiper les tentatives d'attaque ;
- cas de multiples opérations sensibles (multiple delete, multiple download) ;
- synchronisations (Messagerie, OneDrive…) avec des nouveaux appareils.

Il est conseillé de revoir régulièrement les droits accordés aux applications Office 365 et celles qui sont intégrées à Azure Active Directory.

La messagerie est particulièrement à surveiller pour détecter les signaux faibles de phishing réussis. Cette surveillance doit se focaliser sur les opérations pouvant signifier qu'un phishing a été réussi, comme :

- les règles d'inbox ayant une action de transfert vers l'extérieur ou vers le dossier RSS ;
- les règles de suppression de certains messages avec un objet spécifique (à faire valider par l'utilisateur concerné) ;
- les changements de permission (atypiques) sur une boîte aux lettres (à faire valider par l'utilisateur concerné) ;
- un volume d'activité inhabituel (nombre de messages émis, nombre de fichiers téléchargés…) ;
- des partages inhabituels sur OneDrive, Teams ou SharePoint.

IV.5.3. CMD-3 Monitorer les accès aux données

Le dernier niveau de surveillance concerne l'accès aux contenus d'Office 365, en particulier les documents stockés ou partagés par les utilisateurs. Les scénarios d'accès jugés contraires à la sécurité de l'organisation doivent être surveillés.

La liste ci-dessous présente des exemples que chaque organisation doit contextualiser :

- identifier tout nouveau partage (interne, externe, anonyme) et, en fonction de sa sensibilité et de la politique de sécurité, le faire valider par le propriétaire ;
- contrôler la modification et la suppression de documents sensibles (classifier confidentiel, stocker dans un partage sensible…) ;
- détecter l'ajout de membres dans les groupes sensibles (groupes AD, groupes Office 365, groupe de groupes…) ;
- surveiller les changements de propriétaire (Teams, SharePoint…) ;
- détecter les délégations et partages pour les comptes "Défaut" et "Anonyme" et générer une alerte vers les équipes d'administration ou sécurité opérationnelle.

Il est préconisé de mettre en place un processus de notification des utilisateurs afin de faciliter la levée de doutes sur certaines opérations et ainsi responsabiliser les propriétaires des partages et documents sensibles. Le Propriétaire d'un partage, qui connaît ses membres, doit être en mesure de confirmer le changement ou de retirer l'utilisateur ou le groupe concerné de la liste des membres autorisés. Cependant il faut éviter de « spammer » un utilisateur. C'est pourquoi il est préférable d'utiliser une solution permettant la création de profils utilisateurs et la mise à jour permanente de ces profils en fonction des cas rencontrés et des réponses des utilisateurs.

Il est recommandé d'automatiser les revues d'habilitation et d'effectuer à fréquence régulière des campagnes invitant chaque propriétaire à valider les délégations et les membres des partages (OneDrive, Teams, SharePoint).

Certaines solutions de détection sont en capacité de générer des rapports d'audit précis et individuels sur les usages, les droits, délégations et accès accordés ou effectués sur les ressources du locataire (tenant) Office 365 par chaque utilisateur.

Certaines solutions construisent un profil individuel pour chaque utilisateur après une phase d'apprentissage s'appuyant sur de l'IA et sur de l'analyse comportementale. Ces solutions savent gérer des campagnes automatisées de certification des droits, délégations et accès.

IV.6. Mesures de protection contre les risques réglementaires

IV.6.1. CMR-1 Comprendre les exigences de conformité du fournisseur Microsoft

Pour être en mesure de mettre à disposition un service dans un pays, le fournisseur de cloud (Microsoft) est dans l'obligation de respecter la législation du pays et donc l'ensemble des exigences légales que ce dernier impose. C'est également le cas des législations qui s'imposent aux pays, par exemple à travers des directives européennes qui sont déclinées ensuite dans les lois du pays, comme le RGPD.

Ces aspects réglementaires sont détaillés dans les contrats comme dans l'extrait ci-dessous :

« Microsoft s'engage à se conformer à toutes les lois et réglementations applicables à la fourniture des services en ligne, y compris à la législation relative à la notification des violations de sécurité et aux obligations de protection des données. Cependant, Microsoft n'est pas responsable du respect de toute loi ou réglementation applicable au client ou au secteur d'activité du client qui ne serait pas généralement applicable aux prestataires de services informatiques. Microsoft ne détermine pas si les Données Client incluent des informations soumises à une LOI ou réglementation spécifique ».

« Le client est tenu de se conformer à toutes les lois et réglementations applicables à son utilisation des services en ligne, y compris aux lois concernant les données biométriques, la confidentialité des communications ainsi qu'aux obligations de protection des Données ».

Cependant il est de la responsabilité du client (utilisateur du service) de s'assurer qu'il respecte lui-même les réglementations applicables de son pays. En effet, Microsoft n'a pas connaissance des données du client qui sont stockées ou traitées dans le service Office 365 et peuvent être soumises à des réglementations particulières du fait de leur nature ou de leur sensibilité. Par exemple, le client peut vouloir stocker des données financières ou des données de santé qui sont soumises à des exigences particulières. Il est donc important **que le client soit en mesure d'identifier quelles sont les données sensibles** qui pourraient être stockées ou traitées par le service Office 365 et lui appliquer si nécessaire des contrôles de sécurité supplémentaires (chiffrement, anonymisation, authentification renforcée, etc..) pour être en conformité avec la réglementation.

L'exemple du RGPD est représentatif car il impose que le service Office 365 respecte les exigences du RGPD en tant que sous-traitant (ce qui est obligatoire), mais impose également des exigences au client en tant que responsable du traitement. On peut citer l'autre exemple des données de santé, où les services en ligne de Microsoft sont certifiés Hébergeur de Données de Santé (HDS), mais où le client a en charge de mettre en place les contrôles de sécurité nécessaires (inclus nativement dans la plateforme Office 365) pour garantir le niveau de protection nécessaire pour le stockage et le traitement des données de santé.

Liens utiles :

Prendre en compte l'arrêt Schrems II	https://www.cnil.fr/fr/les-clauses-contractuelles-types-de-la-commision-europeenne
Addendum sur la Protection des Données pour les Services en Ligne	https://www.microsoft.com/fr-fr/licensing/product-licensing/products

Microsoft juillet 2020/Online Services Data Protection Addendum (DPA)	
Microsoft compliance offerings	https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide

IV.6.2. CMR-2 Prendre en compte des réglementations nationales spécifiques et sectorielles

Certaines entreprises d'importance vitale (opérateur d'importance vitale ou OIV) sont soumises à la loi de programmation militaire (LPM) qui impose des exigences particulières sur certaines parties de leur système d'information appelées SIIV (système d'information d'importance vitale). Tout OIV a une obligation de déclaration auprès de l'ANSSI et doit donc vérifier si les services d'Office 365 font ou non partie d'un SIIV. Si les services Office 365 ne sont pas dans le périmètre du SIIV, les contraintes de la LPM ne s'appliquent pas. Sinon, une solution de type on-premises pour les parties soumises à la LPM serait une option.

La démarche n'est pas la même concernant les opérateurs de service essentiels en ce qui concerne leur SIE (système d'information essentiel) qui sont soumis à la directive NIS dont les exigences sont proches de la LPM dans l'état actuel du droit, mais préconisant (ENISA) le stockage sur le cloud si les données sont chiffrées au repos, chiffrées quand elles sont transportées et les utilisateurs authentifiés. Dans ce cas, les règles vues en IV.4.1 s'appliquent.

Pour les autres réglementations, il est nécessaire d'identifier si certaines des données traitées ou stockées sont soumises à des exigences particulières comme des données personnelles (par exemple le RGPD) ou des données médicales, bancaires, etc. qui imposeraient des mesures de protection particulières.

Dans le cas des données de santé, Office 365 est certifié « hébergeur de données de santé » (HDS) sur les 6 niveaux disponibles et cela n'implique **aucun surcoût** pour le client. Le certificat est disponible sur le site du BSI (British Standards Institution), l'organisme certificateur.

Vous pourrez ensuite faire le choix, soit de ne pas stocker ou faire transiter ces données dans Office 365 (à vous de les identifier), soit de leur appliquer des protections particulières en utilisant les solutions de chiffrement disponibles sur la plateforme Office 365 (avec des options comme l'utilisation de vos propres clés de chiffrement), soit d'utiliser des solutions tierces.

Il faut noter que l'utilisation d'un surchiffrement a l'avantage de rendre les données totalement indéchiffrables par le service Office 365, mais au prix de pertes de fonctionnalités : vous perdez les fonctions de collaboration, de eDiscovery dans le cadre d'actions légales, de détection anti-malware, d'indexation et de recherche natives. Certaines solutions tierces vous permettent de conserver des fonctions d'indexation pour rechercher des documents et les métadonnées utiles pour le fonctionnement des workflows.

Il est important également de ne pas s'appliquer des contraintes supplémentaires par méconnaissance des réelles exigences réglementaires ou pour « faire mieux », ceci impliquant inévitablement des surcoûts.

Liens utiles

Hébergeur de données de santé	https://docs.microsoft.com/fr-fr/microsoft-365/compliance/offering-hds-france
Liste des hébergeurs certifiés	https://esante.gouv.fr/labels-certifications/hds/liste-des-herbergeurs-certifies
Certificat HDS	https://www.bsigroup.com/en-GB/our-services/certification/certificate-and-client-

	directory/search-results/?searchkey=licence%3d701569%26company%3dmicrosoft&licencenumber=HDS%20701569
Pour une liste exhaustive des certifications de la plateforme Office 365 : Microsoft compliance offerings	https://docs.microsoft.com/en-us/microsoft-365/compliance/offering-home?view=o365-worldwide

Note sur SecNumCLoud

De même que des certifications de type ISO 27001, la certification SecNumCloud n'est pas une obligation légale et n'est donc pas traitée dans cette section.

IV.6.3. CMR-3 Comprendre les risques liés aux réglementations et aux engagements du fournisseur de cloud

Avant de prendre des décisions engageantes, assurez-vous que vous avez une bonne compréhension des réglementations qui s'appliquent à votre organisation. Rapprochez-vous de vos équipes juridiques ou faites appel à des juristes pour être assurés de disposer d'informations de confiance et non d'avis ou d'interprétations biaisés.

Vous trouverez ci-dessous des informations sur des questions récurrentes.

Rappel sur le CLOUD Act

Il est important de clarifier le fait que le CLOUD Act (Clarifying Lawful Overseas Use of Data Act) n'autorise pas un accès incontrôlé et illimité du gouvernement américain aux données stockées en dehors des États-Unis.

Le CLOUD Act est un mécanisme procédural permettant aux autorités chargées de l'application des lois de demander aux fournisseurs de services cloud de communiquer des données sous leur contrôle, y compris lorsque les données sont hébergées en dehors du territoire américain, dans le cadre de poursuites pénales. Ces demandes doivent être examinées et approuvées par un juge indépendant après avoir établi des faits spécifiques démontrant la cause probable d'un crime.

Les engagements contractuels qui existaient avant le CLOUD Act restent inchangés. Ils font partie du contrat standard actuel (Conditions des services en ligne – Divulgation des données traitées) et constituent une garantie juridique concrète pour les clients.

Divulgation des données traitées

Microsoft s'engage contractuellement à ne pas divulguer les données traitées aux pouvoirs publics, sauf si elle y est tenue par la loi. Dès réception d'une demande et après examen, si la demande est valable, Microsoft s'efforcera de rediriger la demande directement au client.

Microsoft ne saurait fournir à un tiers un accès direct, indirect, général ou illimité aux données traitées ou les clés de chiffrement utilisées pour les sécuriser.

Transparence sur les requêtes en provenance des forces de l'ordre

À des fins de transparence, Microsoft publie tous les six mois des rapports sur les demandes d'application de la loi. Ces rapports incluent le nombre de demandes reçues par Microsoft tous pays confondus.

Pour plus d'informations

Termes des contrats de licence/Addendum sur la Protection des données pour les services en ligne Microsoft janvier 2020/Online Services Data Protection Addendum (DPA)	https://www.microsoft.com/fr-fr/licensing/product-licensing/products
Law Enforcement Requests Report	https://www.microsoft.com/en-us/corporate-responsibility/law-enforcement-requests-report

IV.7. Tableau de synthèse

Risques SaaS	Mesures simples	Mesures moyennes	Mesures complexes
RS01 Vol et Usurpation d'identité	CMI–1 Mettre en place une authentification renforcée		
		CMD-2 Monitorer les usages	
RS02 Non-maîtrise de la réversibilité		CMG-8 Maîtriser les transferts de données (Réversibilité)	
RS03 Mauvaise gestion des identités et des accès		CMI–3 Mettre en place une revue des comptes et privilèges	
		CMD-3 Monitorer les accès aux données	
RS04 Fuite de données incontrôlées	CMP-2 Protéger les informations sensibles par chiffrement		
		CMD-2 Monitorer les usages	
RS05 Modification majeure des fonctionnalités	CMG-1 Veiller à la mise à jour Office 365		
		CMG-8 Maîtriser les transferts de données (réversibilité)	
RS06 Saturation réseau à la suite d'une évolution des usages	CMH-9 Surveiller les performances des infrastructures d'accès et augmenter la bande passante si nécessaire		
RS07 Altération/Perte de données		CMG-3 Définir une stratégie de rétention des données	
		CMD-3 Monitorer les accès aux données	
RS08 Indisponibilité du service	CMH-8 Faciliter le travail en mode déconnecté		
		CMH-11 Déterminer l'indisponibilité effective du service Office 365	
		CMI–5 Maîtriser les appareils autorisés à accéder à Office 365	
Risques Appareil	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RA01 Usage depuis un appareil compromis	CMH-1 S'équiper contre les codes malveillants		
	CMP-2 Protéger les informations sensibles par chiffrement		
		CMP-5 Gérer les applications avec un outil de gestion des applications mobiles	
		CMP-6 Mettre en place le contrôle d'accès conditionnel	
		CMD-3 Monitorer les accès aux données	
RA02 Usage depuis un appareil perdu/volé		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
	CMI–1 Mettre en place une authentification renforcée		

		CMI–5 Maîtriser les appareils autorisés à accéder à Office 365	
	CMP-2 Protéger les informations sensibles par chiffrement		
		CMP-6 Mettre en place le contrôle d'accès conditionnel	
	CMP-7 Interdire la synchronisation des données depuis les appareils non gérés		
RA03 Usage depuis un appareil non maîtrisé		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
	CMG-6 Mettre en place une gestion stricte des licences		
		CMI–5 Maîtriser les appareils autorisés à accéder à Office 365	
		CMP-5 Gérer les applications avec un outil de gestion des applications mobiles	
		CMP-6 Mettre en place le contrôle d'accès conditionnel	
		CMD-3 Monitorer les accès aux données	
Collaboration	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RC01 Fuite *via* des partages trop permissifs		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
		CMH-2 Durcissement des configurations des services de collaboration	
		CMD-3 Monitorer les accès aux données	
RC02 Mauvaise gestion des groupes Office 365	CMI–2 Mettre en place une gestion des arrivées/départs		
		CMD-3 Monitorer les accès aux données	
RC03 Mauvaise gestion des permissions sur un partage		CMD-3 Monitorer les accès aux données	
		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
RC04 Fuite *via* le partage d'un lien anonyme		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
	CMH-2 Durcissement des configurations des services de collaboration		
		CMD-2 Monitorer les usages	
		CMD-3 Monitorer les accès aux données	
RC05 Diffusion de fichiers malveillants		CMP-6 Mettre en place le contrôle d'accès conditionnel	
RC06 Usage non conforme à la charte		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	

Communication	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RM01 Redirection malveillante de messages		CMH-3 Durcissement des configurations des services de messagerie	
		CMD-2 Monitorer les usages	
RM02 Ingénierie sociale (phishing) ciblée Office 365		CMH-3 Durcissement des configurations des services de messagerie	
		CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité	
		CMD-2 Monitorer les usages	
RM03 Délégation non maîtrisée par l'utilisateur		CMH-3 Durcissement des configurations des services de messagerie	
		CMD-2 Monitorer les usages	
RM04 Usurpation de domaine de messagerie		CMH-3 Durcissement des configurations des services de messagerie	
RM05 Fuite de données *via* un service tiers	CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité		
	CMP-2 Protéger les informations sensibles par chiffrement		
	CMP-3 Limiter les droits d'accès aux documents partagés en externe		
RM06 Utilisation d'anciens protocoles (IMAP, POP3)		CMH-3 Durcissement des configurations des services de messagerie	
		CMP-6 Mettre en place le contrôle d'accès conditionnel	
		CMD-2 Monitorer les usages	
RM07 Mauvaise configuration de la rétention (messagerie)		CMH-3 Durcissement des configurations des services de messagerie	
Développement	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RD01 Secrets d'authentification non protégés		CMG-5 Former les administrateurs et les développeurs	
		CMH-4 Durcissement des configurations des développements	
RD02 Mauvaise gestion des droits		CMG-5 Former les administrateurs et les développeurs	
		CMD-1 Monitorer les modifications de configuration	
		CMD-3 Monitorer les accès aux données	
RD03 Mauvais paramétrage OAuth		CMG-5 Former les administrateurs et les développeurs	
		CMD-1 Monitorer les modifications de configuration	

		CMD-3 Monitorer les accès aux données	
RD04 Fuite par détournement de fonctionnalité	CMG-1 Veiller à la mise à jour Office 365		
	CMP-2 Protéger les informations sensibles par chiffrement		
		CMD-2 Monitorer les usages	
Bureautique	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RB01 Exécution de codes malveillants	CMG-1 Veiller à la mise à jour Office 365		
	CMH-1 S'équiper contre les codes malveillants		
RB02 Incompatibilité à la suite d'une mise à jour	CMG-1 Veiller à la mise à jour Office 365		
RB03 Non-maîtrise des données utilisées par les fonctions avancées		CMH-5 Durcissement des configurations des services bureautique (expériences connectées, télémétrie…)	
RB04 Non-maîtrise des compléments	CMG-4 Sensibiliser les utilisateurs sur les bonnes pratiques de sécurité		
	CMI–6 Mettre en place un processus de gestion des services tiers		
Gestion du locataire (tenant)	**Mesures simples**	**Mesures moyennes**	**Mesures complexes**
RG01 Mauvaise gestion des départs et des arrivées		CMI–2 Mettre en place une gestion des arrivées/départs	
		CMP-4 Définir un processus de récupération des données	
	CMG-3 Définir une stratégie de rétention des données		
RG02 Mauvaise gouvernance des services	CMG-1 Veiller à la mise à jour Office 365		
	CMG-6 Mettre en place une gestion stricte des licences		
	CMG-7 Mettre en place un processus de sélection et de configuration des services		
			CMH-6 S'outiller pour mieux gérer son locataire (tenant) (pour grandes organisations)
		CMD-1 Monitorer les modifications de configuration	

RG03 Perte de traçabilité des actions des administrateurs		CMI–3 Mettre en place une revue des comptes et privilèges	
RG04 Non-ségrégation de l'administration	CMG-2 Définir un modèle de rôles sécurisé		
	CMG-5 Former les administrateurs et les développeurs		
		CMI–3 Mettre en place une revue des comptes et privilèges	
RG05 Absence de surveillance des comptes à privilèges		CMD-1 Monitorer les modifications de configuration	
		CMI–3 Mettre en place une revue des comptes et privilèges	
RG06 Non-adéquation de l'équipe d'administration	CMG-5 Former les administrateurs et les développeurs		
	CMI–1 Mettre en place une authentification renforcée		
RG07 Administration depuis un appareil compromis	CMG-5 Former les administrateurs et les développeurs		
			CMH-10 Mettre en œuvre des stations d'administration sécurisées et dédiées (PAW)
		CMI–5 Maîtriser les appareils autorisés à accéder à Office 365	
		CMP-6 Mettre en place le contrôle d'accès conditionnelCMD-1 Monitorer les modifications de configuration	
RG08 Erreur/méconnaissance de l'administrateur	CMG-5 Former les administrateurs et les développeurs		
		CMG-8 Maîtriser les transferts de données (Réversibilité)	
		CMH-7 Documenter la gestion du locataire (tenant)	
		CMD-1 Monitorer les modifications de configuration	
RG09 Fédération d'identités mal maîtrisée (Azure AD)		CMI–4 : Assurer la disponibilité de l'authentification en mode fédéré	
RG10 Mauvaise gestion des clés du locataire (tenant) par l'organisation			CMP-8 Respecter les bonnes pratiques liées à l'utilisation de Customer Key
RG11 Non-maîtrise des montées de version des services	CMG-1 Veiller à la mise à jour Office 365		
	CMG-4 Sensibiliser les utilisateurs sur les		

RG12 Mauvaise gestion des droits donnés aux invités	bonnes pratiques de sécurité		
	CMI–2 Mettre en place une gestion des arrivées/départs		
		CMI–7 Implémenter un cycle de vie des utilisateurs invités	
		CMP-3 Limiter les droits d'accès aux documents partagés en externe	
		CMD-3 Monitorer les accès aux données	
		CMP-6 Mettre en place le contrôle d'accès conditionnel	
Lois			
RL01 Non-conformité réglementaire	CMG-3 Définir une stratégie de rétention des données		
	CMP-1 Classifier les documents et messages		
	CMP-2 Protéger les informations sensibles par chiffrement		
		CMD-3 Monitorer les accès aux données	
	CMR-1 Comprendre les exigences de conformité du fournisseur Microsoft		
		CMR-2 Prendre en compte des réglementations nationales spécifiques et sectorielles	
		CMR-3 Comprendre les risques liés aux réglementations et aux engagements du fournisseur de cloud	

V. Index références Web

VI. Glossaire

- **API (Application Programming Interface) :** ensemble normalisé de classes, de méthodes, de fonctions et de constantes par laquelle un logiciel offre des services à d'autres logiciels. Elle est offerte par une bibliothèque logicielle ou un service Web, le plus souvent accompagnée d'une description qui spécifie comment des programmes consommateurs peuvent se servir des fonctionnalités du programme fournisseur.
- **API REST :** style architectural et méthodologie fréquemment utilisés dans le développement de services Internet, tels que les systèmes hypermédias distribués. Par exemple, lorsqu'un développeur demande à l'API Twitter de récupérer l'objet d'un utilisateur (une ressource), l'API renvoie l'état de cet utilisateur, son nom, ses abonnés et les publications partagées sur Twitter.
- **ATAWAD (Any Time Any Where Any Device) :** possibilité de se connecter quel que soit le lieu, le moment ou l'appareil/support utilisé.
- **ATP (Advanced Threat Prevention) :** détecte, analyse et stoppe les menaces provenant de programmes malveillants qui ont évolué pour contourner les méthodes de sécurité traditionnelles.
- **Azure Active Directory (Azure AD) :** est le service de gestion de l'accès et des identités basé sur le cloud de Microsoft. Il ne doit pas être confondu avec le service d'annuaire Active Directory (nom complet Active Directory Domain Services) qui est un annuaire LDAP déployé en interne qui est un référentiel d'identité et qui assure l'authentification, la gestion des objets informatiques, la stratégie de groupe et les relations d'approbation.
- **Blob Azure :** solution de stockage d'objet de Microsoft pour le cloud. Le stockage Blob est optimisé pour stocker de grandes quantités de données non structurées. Les données non structurées sont des données qui n'obéissent pas à un modèle ou une définition de données en particulier, comme des données texte ou binaires.
- **Click-to-Run :** programme conçu par Microsoft dans le but d'installer votre version d'Office sur votre ordinateur personnel ou professionnel.
- **CNIL (Commission nationale de l'informatique et des libertés) :** autorité chargée de veiller à ce que l'informatique soit au service du citoyen et qu'elle ne porte atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.
- **DNS (Domain Name System) :** service informatique distribué utilisé pour traduire les noms de domaine Internet en adresse IP.
- **DDOS (Distributed Denial Of Service) :** attaque informatique ayant pour but de rendre indisponible un service, d'empêcher les utilisateurs légitimes d'un service de l'utiliser.
- **Espace de travail numérique** (Digital Workplace)
- **EDR :** technologie émergente de détection/protection des menaces sur les EndPoints (ordinateurs, serveurs).
- **Fédération d'identité (service de) :** concept qui vise à mettre en place une centralisation des données, notamment des données d'identité, au sein d'un domaine informatique. Ainsi, un utilisateur ne se connectera qu'une unique fois par session auprès d'une structure reconnue qui lui fournira la preuve de son identité.
- **FIDO2 :** projet de la FIDO Alliance dont l'objectif est de standardiser les processus d'authentification sécurisés et sans mot de passe. Cette initiative s'appuie sur 2 protocoles travaillés avec le World Wide Web Consortium (W3C) WebAuthn et CTAP. WebAuthn

propose une interface d'authentification des utilisateurs aux applications Web à l'aide de clés asymétriques ; CTAP permet à des équipements externes tels que des terminaux mobiles ou des clés de sécurité FIDO de travailler avec les navigateurs supportant WebAuthn, mais aussi de faire office d'authentificateur pour des applications sur ordinateur ou des services Web.

- **GDPR ou RGPD en Français :** règlement de l'Union européenne qui constitue le texte de référence en matière de protection des données à caractère personnel. Il régule notamment le fait que des données personnelles soient stockées à l'étranger.
- **Hameçonnage (phishing) :** message ou site Web usurpant une identité de confiance utilisé pour inciter un utilisateur à cliquer sur un lien l'amenant à révéler ses identifiants
- **HSM (Hardware Security Module) :** matériel électronique offrant un service de sécurité qui consiste à générer, stocker et protéger des clés cryptographiques.
- **IAM (Identity Access Management)** ou Gestion des identités et des accès : ensemble des processus mis en œuvre par une entité pour la gestion des habilitations de ses utilisateurs à son système d'information ou à ses applications. Il s'agit donc de gérer qui a accès à quelle information à travers le temps.
- **ISP (Internet Service Provider) :** fournisseurs d'accès Internet.
- **Malware :** programme développé dans le but de nuire à un système informatique, sans le consentement de l'utilisateur dont l'ordinateur est infecté.
- **MAM (Mobile Application Management) :** permet de sécuriser, gérer et distribuer les applications mobiles sur les appareils mobiles. Ces logiciels peuvent être utilisés aussi bien sur des équipements appartenant à l'entreprise que ceux des personnes externes à la société.
- **MDM (Mobile Device Management) également appelé EMM et UEM :** outil de gestion de flotte d'appareils mobiles (smartphones, tablettes ou PC portables).
- **MFA (Multi Factor Authentication) :** authentification à facteurs multiples est une méthode d'authentification dans laquelle un utilisateur n'est autorisé à accéder à un site Web ou à une application qu'après avoir présenté avec succès deux ou plusieurs éléments de preuve (ou facteurs) à un mécanisme d'authentification.
- **Microsoft 365 Apps for Enterprise :** nouveau nom de la suite Office Pro Plus (Word, Excel, PowerPoint, Outlook…).
- **Microsoft Teams :** est un outil de réunion en visioconférence et de collaboration qui agrège les services Office 365.
- **Microsoft Power Apps :** ne suite d'applications, de services, de connecteurs et une plateforme de données qui fournissent un environnement de développement applicatif dans le but de concevoir des applications.
- **Microsoft Power BI :** solution de Business Intelligence développée par Microsoft pour permettre aux entreprises d'agréger, d'analyser et de visualiser les données en provenance de sources multiples.
- **Microsoft PowerShell :** suite logicielle développée par Microsoft qui intègre une interface en ligne de commande, un langage de script nommé PowerShell ainsi qu'un kit de développement.
- **OAuth :** protocole libre qui permet d'autoriser un site Web, un logiciel ou une application (dite « consommateur ») à utiliser l'API sécurisée d'un autre site Web (dit « fournisseur ») pour le compte d'un utilisateur. OAuth n'est pas un protocole d'authentification, mais de « délégation d'autorisation ».

- **Outlook Web Access :** permet aux usagers d'accéder à leur courrier électronique à l'aide d'un navigateur Web, en évitant la procédure préalable d'installation requise par Microsoft Outlook.
- **Partage :** espace collaboratif (Teams, SharePoint) ou répertoire (One Drive).
- **Politique de protection contre la fraude à messagerie :** première ligne de défense contre les courriers électroniques d'imposteurs doit être l'authentification des messages, pas les utilisateurs. Pour l'authentification des messages, vous devez implémenter trois normes dont l'importance est cruciale pour toute organisation : SPF, DKIM, DMARC.
- **Politique SPF (Sender Policy Framework) :** norme SPF est un protocole d'authentification des messages qui permet à votre entreprise de spécifier qui est autorisé à utiliser votre domaine pour envoyer des messages.
- **Politique DKIM (DomainKeys Identified Mail) :** norme d'authentification fiable du nom de domaine de l'expéditeur d'un courrier électronique. Elle constitue une protection efficace contre le spam et l'hameçonnage. DKIM fonctionne par signature cryptographique du corps du message ou d'une partie de celui-ci et d'une partie de ses en-têtes. Une signature DKIM vérifie donc l'authenticité du domaine expéditeur et garantit l'intégrité du message.
- **Politique DMARC (Domain-based Message Authentication Reporting and Conformance) :** politique qui autorise l'expéditeur à indiquer que ses messages sont protégés par SPF et/ou DKIM et indique au destinataire ce qu'il doit faire si ces méthodes d'authentification échouent.
- **Rançongiciel ou ransomware :** logiciel malveillant qui prend en otage des données d'une organisation ou des données d'un utilisateur. Pour ce faire, un rançongiciel chiffre des données puis demande à leur propriétaire d'envoyer de l'argent en échange de la clé qui permettra de les déchiffrer.
- **RBAC (Role Based Access Control) :** modèle de contrôle d'accès à un système d'information dans lequel chaque décision d'accès est basée sur le rôle auquel l'utilisateur est associé.
- **Sandboxing :** mécanisme de sécurité informatique se basant sur l'isolation de composants logiciels, de logiciels ou de groupes de logiciels par rapport à leur logiciel ou système d'exploitation hôte. L'isolation a pour rôle de permettre l'exécution du ou des composants logiciels en diminuant les risques liés à cette exécution pour l'hôte.
- **SIEM (Security Incident & Event management)** ou Gestion des incidents et des événements de sécurité : outil permettant de détecter, puis traiter les événements de sécurité du système d'information (SI) en appliquant des règles d'agrégation et de corrélation sur les logs dans le but de détecter des attaques.
- **Spear Phishing :** variante informatique de l'hameçonnage épaulée par des techniques d'ingénierie sociale. Contrairement à l'hameçonnage traditionnel basé sur l'envoi d'un message générique à un grand nombre de destinataires, le spear phishing se focalise sur un nombre limité d'utilisateurs (souvent un seul) auxquels est envoyé un message fortement personnalisé.
- **SSO (Single Sign On) :** permet de s'authentifier une seule fois et d'accéder à plusieurs applications.
- **Stratégie de Litigation Hold :** stratégie de conservation pour litige permettant de préserver tout le contenu de la boîte aux lettres, y compris les éléments supprimés et les versions originales des éléments modifiés.

- **Stratégie de Place Hold :** stratégie définie par l'administrateur permettant de préserver tout le contenu de la boîte aux lettres, y compris les éléments supprimés et les versions originales des éléments modifiés.
- **Tenant (ou locataire) :** un tenant Azure regroupe les services Microsoft faisant l'objet d'un contrat avec l'organisation, incluant un service annuaire (Azure AD) et les services SaaS, (en particulier Office 365), PaaS et IaaS souscrits par l'organisation.
- **SaaS ou offre cloud SaaS :** solution hébergée et maintenue par un hébergeur, ici Microsoft qui assure son fonctionnement selon un certain niveau de disponibilité. Le paramétrage fonctionnel est réalisé par l'organisation.
- **VPN (Virtual Private Network) :** système permettant de créer un lien direct entre des ordinateurs distants, qui isole leurs échanges du reste du trafic se déroulant sur des réseaux de télécommunication publics.

et sécurité

L'ESPRIT D'ÉCHANGE

11 rue de Mogador
75009 Paris
France
+33 1 53 25 08 80
clusif@clusif.fr

Téléchargez toutes les productions du Clusif sur

clusif.fr