Chapitre 5
Protection des données

1. Introduction

Toujours dans notre aventure **Zero Trust,** après avoir renforcé l'identité, réduit la surface d'attaque et déployé des outils de détection, prévention et protection, nous nous concentrerons ici sur l'aspect "donnée" et sa protection.

Le but est de protéger la donnée contre la fuite mais surtout d'en garder le contrôle si celle-ci venait à être volée et divulguée à l'extérieur de l'organisation.

Comme on peut le constater de nos jours, les attaquants se servent des données d'entreprise ou de particulier à des fins financières, pour les revendre sur Internet.

L'enjeu ici est très important, il est nécessaire et primordial d'investir du temps et de l'argent afin de sécuriser ses données. Dans son offre de sécurité, Microsoft intègre non seulement la sécurité globale que nous avons abordée précédemment avec l'offre Microsoft 365 Defender et Azure Defender, mais aussi la protection et le contrôle de données avec la suite Microsoft Information Protection.

2. Microsoft Information Protection

(MIP) Microsoft Information Protection est un ensemble d'outils qui proviennent du plan Conformité Microsoft 365. Cette suite d'outils et de fonctionnalités offre les possibilités suivantes pour sécuriser et contrôler la donnée dans un système d'information :

- **Évaluation des données** : vous permet de mieux connaître vos données, leur type, leur sensibilité et surtout de définir les plus critiques. Vous pouvez, à cet effet, utiliser par exemple les types d'informations sensibles qui consistent à identifier les données à l'aide d'expressions régulières proposées par Microsoft ou alors personnalisées par vos soins. Cette partie propose également les classifieurs entraînables ou encore la classification des données.
- **Protection des données** : il s'agit de plusieurs outils qui vont permettre de protéger les données avec des mécanismes de chiffrement et l'intégration avec Cloud App Security. On retrouve ici par exemple les étiquettes de confidentialité, le chiffrement à double clé, le chiffrement de message Office 365 ou encore le scanner d'étiquettes.
- **Protection contre la fuite** : des outils sont aussi disponibles pour cette partie qui permettent de protéger le système d'information contre la fuite de données vers l'extérieur avec l'offre DLP Microsoft ou encore la protection contre la perte de données sur les stations de travail.

Dans le cadre de notre stratégie Zero Trust, nous allons traiter des fonctionnalités suivantes qui permettent de contrôler, de gouverner et de protéger les données contre le vol :

- Les étiquettes de confidentialité (*Sensitivity Labels* en anglais)
- Le chiffrement à double clé
- La protection contre la perte de données (DLP for Endpoint)

3. Classifier et protéger

3.1 Introduction

Cette partie concerne la classification et la protection des données. Comme vous le savez, nous sommes dans un monde changeant où la mobilité est omniprésente, car les collaborateurs travaillent depuis plusieurs appareils mobiles et voyagent. La crise de la **COVID-19** a accéléré ce phénomène, poussant les utilisateurs à travailler depuis leur domicile. Tous ces changements apportent un challenge de taille à la sécurité de la donnée.

La plupart des entreprises doivent répondre à cette problématique : **comment offrir de la productivité et de la mobilité à mes collaborateurs tout en restant sécurisée ?**

Nous allons aborder dans cette partie les étiquettes de confidentialité (*Sensitivity Labels* en anglais) qui vont permettre de répondre à cette question de manière simple et efficace.

Nous ferons également un peu d'histoire afin de comprendre comment Microsoft est passé d'AD RMS au Sensitivity Label, en passant par Azure RMS et Azure Information Protection.

Azure Information Protection

Un peu d'histoire avant de commencer. Avant que n'apparaissent les solutions cloud, Microsoft offrait et offre toujours la fonctionnalité **AD RMS**, permettant de classifier et de protéger les données On-premises.

Ensuite, avec la venue de Microsoft Azure, Microsoft a sorti le même mécanisme de protection mais pour son offre cloud nommé : Azure RMS (*Azure Right Management Service*).

Suite à cela, Microsoft a souhaité renforcer son offre en apportant de la classification de manière plus visuelle, en achetant l'entreprise **Secure Island**, le produit est alors devenu : Azure Information Protection. Il permet de classifier et de chiffrer les données à l'aide d'un client AIP, offrant aux utilisateurs une expérience riche et fiable.

Avec Microsoft 365, Microsoft a souhaité mutualiser son offre de protection de données avec Microsoft Information Protection et propose les étiquettes de confidentialité qui permettent de faire la même chose qu'Azure Information Protection mais de manière globale. On peut en effet appliquer ces étiquettes de confidentialité sur plusieurs produits Microsoft 365, comme SharePoint Online, Microsoft Teams, Office for Web, Outlook for Web, Outlook for mobile (iOS et Android) Power Bi data, etc.

Microsoft va plus loin avec Azure en étendant cette fonctionnalité grâce à Azure Purview aux services tels qu'Azure SQL, Blob Storage, Data Lake Storage, Azure SQL Database.

Microsoft recommande d'ailleurs la migration de vos étiquettes Azure Information Protection vers les étiquettes de confidentialité. Voici un article officiel de Microsoft qui traite le sujet :
https://techcommunity.microsoft.com/t5/microsoft-security-and/understanding-unified-labeling-migration/ba-p/783185

3.2 Découverte des étiquettes de confidentialité

Nous allons dans cette section aborder les étiquettes de confidentialité (*Sensitivity Labels* en anglais). On verra leur fonctionnement, leur déploiement et leur administration.

3.2.1 Introduction

Les étiquettes de confidentialité peuvent aider les entreprises à classifier et protéger leurs données de manière simple et efficace.

Les étiquettes de confidentialité sont tout simplement des règles de classification et de chiffrement que l'on va appliquer à une audience (groupe Azure Active Directory). Ensuite, les membres de ces groupes vont pouvoir échanger, collaborer en protégeant et classifiant leurs données avec ces étiquettes.

L'utilisateur pourra appliquer une étiquette de confidentialité à son document en fonction de sa nature ou alors celle-ci s'appliquera automatiquement sur le document. Ceci dépend du fonctionnement de l'entreprise et surtout de la nature de ses données.

Ces étiquettes s'intègrent très bien avec la suite Office. L'utilisateur peut aussi les voir dans l'Explorer Windows si ce dernier souhaite protéger des répertoires entiers.

Les étiquettes de confidentialité offrent plusieurs possibilités :

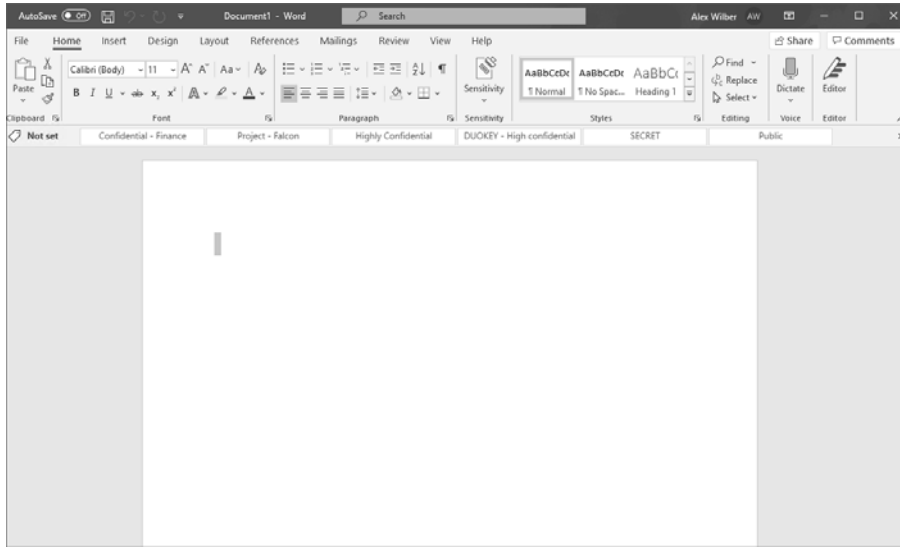
- **Collaboration interne et externe** : les utilisateurs peuvent collaborer avec des fichiers classifiés et/ou chiffrés en interne comme en externe avec des clients et partenaires.
- **Toute plateforme** : les utilisateurs peuvent appliquer les étiquettes de confidentialité sur les applications Office pour Windows 10, Office Web et aussi MacOs, Android et iOS.
- **Multiproduit** : les utilisateurs peuvent appliquer les étiquettes de confidentialité dans Microsoft Teams, les groupes Microsoft 365 et les sites SharePoint Online.
- **Chiffrement à double clé** : les utilisateurs peuvent appliquer les étiquettes de confidentialité avec un chiffrement à double clé afin d'avoir la main sur la master Key.
- **SDK Microsoft Information protection** : avec ce SDK mis à disposition par Microsoft, les utilisateurs peuvent utiliser les étiquettes de confidentialité avec des applications tierces.
- **Intégration d'autres produits** : les étiquettes de confidentialité peuvent être appliquées également dans Power Bi ou encore vers des services PaaS Azure avec Azure Purview.

– **Cloud App Security** : il est possible d'intégrer Cloud App Security et les étiquettes de confidentialité afin de classifier et chiffrer les données via des stratégies.

Pour rappel, une étiquette peut :

– Classifier un document sans apporter de protection, c'est-à-dire que le document est uniquement classifié selon des règles définies par l'entreprise.
– Classifier et chiffrer un document, ici le document est classifié mais surtout chiffré et protégé, ce qui veut dire que seuls les membres autorisés dans la stratégie de l'étiquette pourront consulter le document.

Voici dans la capture ci-dessous un exemple de présence d'étiquette de confidentialité sur la suite Office 365 ProPlus. On peut apercevoir sous le menu à rubans de Word les étiquettes publiées, l'utilisateur n'a plus qu'à sélectionner une étiquette afin de classifier et/ou chiffrer son document :



3.2.2 Prérequis

Licence

Plusieurs plans de licences permettent l'utilisation des étiquettes de confidentialité de manière manuelle :

– Microsoft 365 F1
– Microsoft 365 F3
– Microsoft 365 E3

- Microsoft 365 E5
- Microsoft 365 G3
- Microsoft 365 A5
- Microsoft 365 Business Premium
- Enterprise Mobility + Security E3 / E5 F3
- Office 365 A3/A5/F3/E3/E5
- Azure Information Plan 1 et Plan 2

Les plans suivants peuvent prendre en charge la classification des étiquettes de confidentialité de manière automatique :

- Microsoft 365 E5
- Microsoft 365 A5
- Microsoft 365 G5
- Microsoft 365 A5 / E5 / G5 Compliance
- Microsoft 365 Information Protection et Gouvernance
- Office 365 E5
- Conformité avancée Office 365
- Enterprise Mobility + Security E5
- Azure Information Plan 2

Office

Certaines versions de la suite Office (Microsoft 365 Apps for enterprise provenant des licences Microsoft 365) peuvent prendre en charge les étiquettes de confidentialité de manière intégrée sans besoin d'installation de client Azure Information Protection UL (*Unified Label*).

Si vous possédez des versions MSI office (version On-premises qui s'active avec une licence hors 365) par exemple ici : https://docs.microsoft.com/en-us/deployoffice/install-different-office-visio-and-project-versions-on-the-same-computer, il sera nécessaire d'installer le client Azure Information Protection UL afin de pouvoir afficher les étiquettes sur la suite Office.

Voici l'article officiel de Microsoft qui donne tous les prérequis :
https://docs.microsoft.com/fr-fr/microsoft-365/compliance/sensitivity-labels-office-apps?view=o365-worldwide

Droits

Voici les rôles Azure Active Directory qui permettent de créer et gérer les étiquettes de confidentialité :

- Administrateur général
- Administrateur des données de conformité
- Administrateur de la conformité
- Administrateur sécurité

Machines

Les étiquettes de confidentialité sont supportées sur les systèmes :

- Windows 10
- Windows 8.1
- Windows 8
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 et Windows Server 2012 R2

Mobile

- iPhone/iPad
- Android

3.3 Design

3.3.1 Préparation

Avant de commencer, il est nécessaire de suivre plusieurs étapes qui permettront de mener à bien ce projet de classification et de protection des données.

Voici un exemple qui peut s'appliquer en entreprise :

Phase	Description	Ordre
Découverte	Découvrir la nature des données, étudier et comprendre le type de donnée présent dans le système d'information.	Phase 1
Taxonomie	Définir une taxonomie et une description de vos étiquettes (labels) par exemple : SECRET - PUBLIC - INTERNE – CONFIDENTIEL.	Phase 2