STALTER Claire
N° candidat : 02245165513

Autorisations sur les applications Power Apps et sur leurs sources de données

Compte-rendu

Sommaire

1. Introduction 2
2. Sites SharePoint 2
3. Listes SharePoint 4
4. Applications Microsoft Power Apps 6
5. Power Apps et listes SharePoint 8
6. Microsoft Dataverse 9

1. Introduction

De septembre 2022 à août 2023, j'effectue ma deuxième année de BTS en alternance au Technicentre Industriel SNCF de Rennes. Intégrée au pôle Amélioration Continue et Numérique, je suis chargée de maintenir et développer des solutions logicielles destinées à des agents internes à l'entreprise.

Pour sa transition numérique, SNCF a notamment choisi Microsoft Power Apps, qui permet de concevoir des applications en low-code. Les bases de données compatibles sont très diverses et peuvent aller des fichiers Excel aux tables SQL, en passant par les listes SharePoint. Ce sont ces dernières que nous utilisons le plus souvent, en attendant une transition vers un système plus solide.

Ce document est la synthèse de mon expérience et de mon apprentissage sur la gestion des autorisations dans un environnement Microsoft : droits au sein d'un site SharePoint et de ses listes, droits d'accès aux applications Power Apps, conséquences sur la sécurité et projets futurs.

2. Sites SharePoint

Au niveau national, tout employé SNCF possède un compte Microsoft d'entreprise (identifiant, adresse mail…) et est ce qu'on appelle un « utilisateur Office 365 ». Un groupe Microsoft 365 est créé pour chaque établissement SNCF par des administrateurs, qui ont accès au Centre d'administration Microsoft 365. Un groupe Microsoft 365 est donc constitué d'utilisateurs Office 365.

Lorsqu'un groupe Microsoft 365 est mis en place, divers éléments sont créés automatiquement, dont une boîte de réception Outlook partagée, un calendrier partagé… mais aussi un site SharePoint.

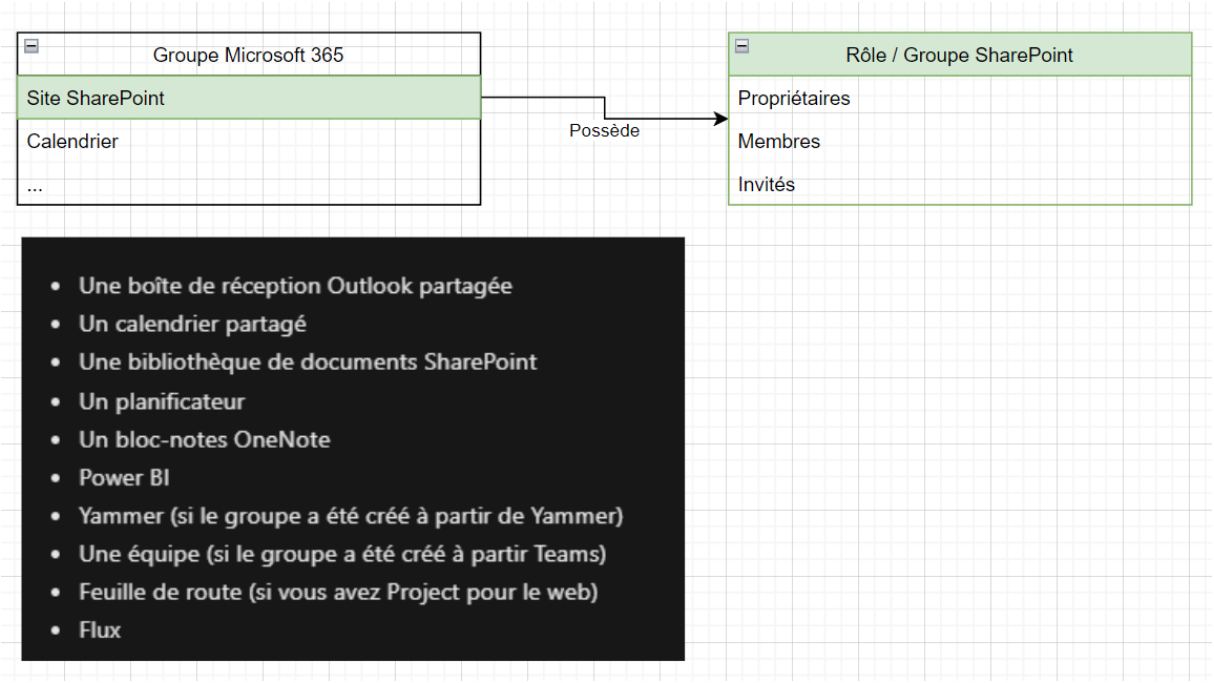

Fig. 1 - Rôles et éléments créés en même temps qu'un groupe Microsoft 365

Un site SharePoint est un espace de travail collaboratif, qui permet essentiellement le partage de documents. Ce site a des membres (les membres du groupe Microsoft 365 associé), qui peuvent avoir différents rôles : propriétaire, membre ou invité. Ces rôles sont créés par défaut, mais les propriétaires ont le pouvoir de créer de nouveaux groupes, pour une gestion des autorisations plus fine.

Ces « propriétaires » ne sont pas les administrateurs. Ils ont en théorie le contrôle sur l'ensemble du site, mais seuls les administrateurs du niveau supérieur ont véritablement le contrôle total. Les propriétaires se comptent sur les doigts d'une main et sont des agents ayant des responsabilités particulières sur le site SharePoint du fait de leur position (directeur d'établissement, responsable numérique).

Différents niveaux d'autorisation existent pour une ressource (le site, mais aussi son contenu comme on le verra plus loin). Là encore, des niveaux d'autorisation par défaut sont fournis avec le site. Cependant, des niveaux d'autorisation particuliers, de type « SNCF – Lecture » ont été créés au niveau national et imposés à tous les établissements.

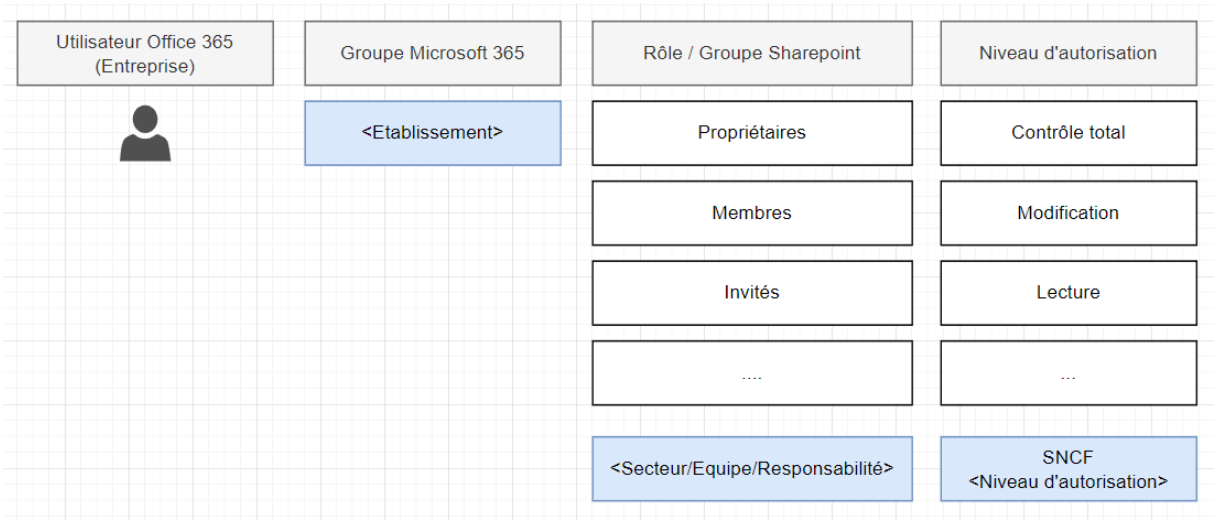

Fig. 2 - Schéma des rôles et niveaux d'autorisation d'un site SharePoint

Les sites SharePoint sont des environnements, des espaces sur des serveurs mis à disposition par la direction du groupe. Ils comprennent :

- des bibliothèques de documents,
- des listes SharePoint,
- des pages,
- éventuellement des sous-sites, qui contiennent eux-mêmes ces éléments.

Les bibliothèques de documents renferment des dossiers et fichiers de toutes sortes : documents textes, images, PDF, etc. Ce sont les listes qui nous intéressent plus particulièrement, car elles peuvent servir de source de données à des applications Power Apps.

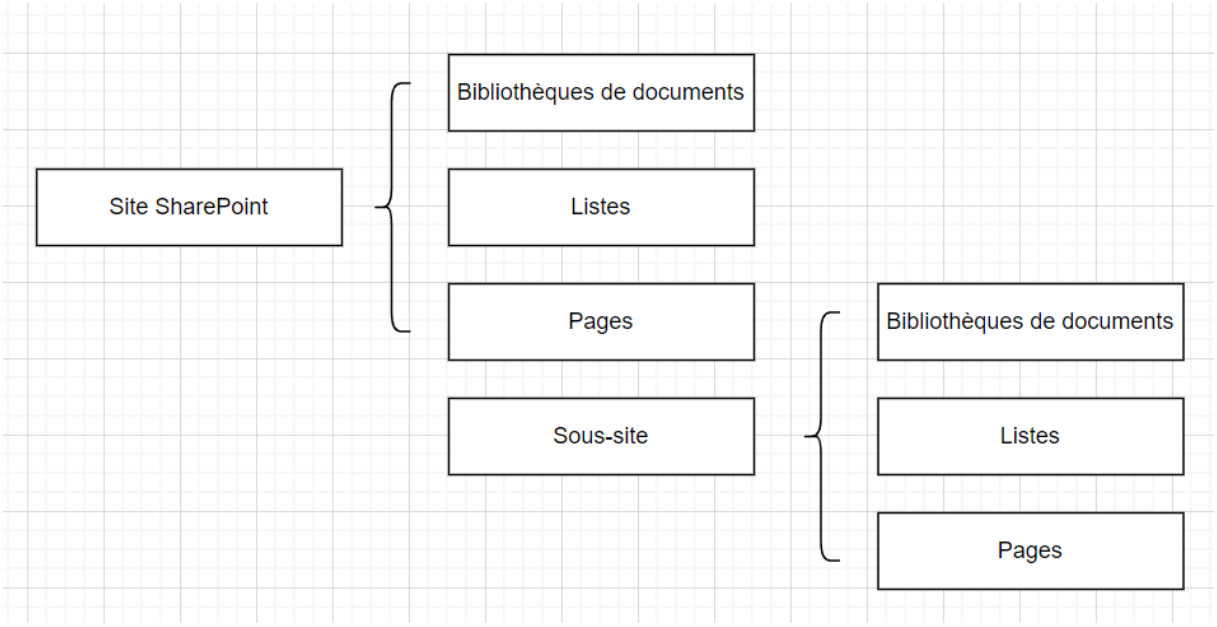

Fig. 3 - Schéma du contenu d'un site SharePoint

3. Listes SharePoint

Les listes SharePoint ne sont ni plus ni moins que des tableaux. Comme dans une table SQL, on y trouve différents champs, de différents types. Chaque ligne, ou enregistrement, est une entrée de la liste possédant un identifiant unique (pas nécessairement visible cependant).

ACNDév_DEMO - Demande Achats ☆

ID+	Date demande	Fournisseur	Equipe	Produit le plus i...	Désignation	Référence four...	Quantité	Demandeur	Pièces jointes	Acheteur en ch...	Urgent
14	21/10/2022	MFI MAINTENANCE FERRI	AC et Num		test dev Claire avec une désignation très longue pour vérifier l'affichage sur différents écrans		5	Claire STALTER	1		Oui
13	20/10/2022	Autre	AC et Num		test dev Claire		3	Claire STALTER			Non
12	19/10/2022	MCSA SET	AC et Num		test dev machinchose		2	Claire STALTER			Oui
11	18/10/2022	AB	AC et Num		test dev Claire nom demandeur		1	Geoffrey C			Non
10	18/10/2022	AB	AC et Num		test dev compte pc018--ffiodf		30	Claire STALTER			Non
9	18/10/2022	ALSTOM	PERF - CBE		test dev compte		1	Claire STALTER			Non
8	13/10/2022	AB	AC et Num		test dev		4	Claire STALTER		Claire STALTER	Non
7	18/10/2022	AB	AC et Num		test dev		3	Claire STALTER			Non
6	18/10/2022	OFFICEXPRESS	AC et Num		test dev casque		5	Claire STALTER			Non
5	18/10/2022	AMITEC	AC et Num	03183557 -- CALIBRE DE \	test dev		2	Claire STALTER		Claire STALTER	Non
4	18/10/2022	AB	AC et Num	07058242 -- SOUPAPE D L	test dev		3	Claire STALTER			Non
3	03/10/2022	AB	AC et Num		test dev		3	Claire STALTER			Non

Fig. 4 - Aperçu d'une liste SharePoint utilisée lors de tests

Les listes sont stockées à la racine d'un site SharePoint, comme représenté sur la figure 3. Tout le monde ne peut pas créer une liste : il faut pour cela des droits particuliers possédés par le rôle Propriétaire. Par défaut, en effet, les membres de l'établissement n'ont qu'un droit de lecture sur l'ensemble du site.

Le contenu du site SharePoint hérite des autorisations du site : par défaut, un membre a donc le même niveau d'autorisation sur tout le contenu du site.

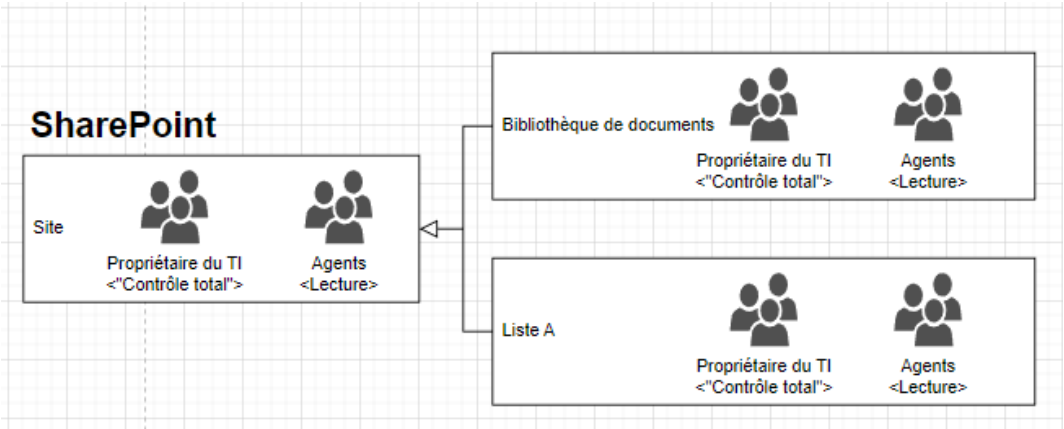

Fig. 5 - Héritage des autorisations sur un site SharePoint

Cela dit, il est possible de « casser l'héritage ». Un niveau d'autorisation particulier peut ainsi être donné à une équipe (un groupe d'utilisateurs Office 365) sur une bibliothèque de documents ou sur une liste. On peut aussi donner un droit spécifique à un utilisateur précis.

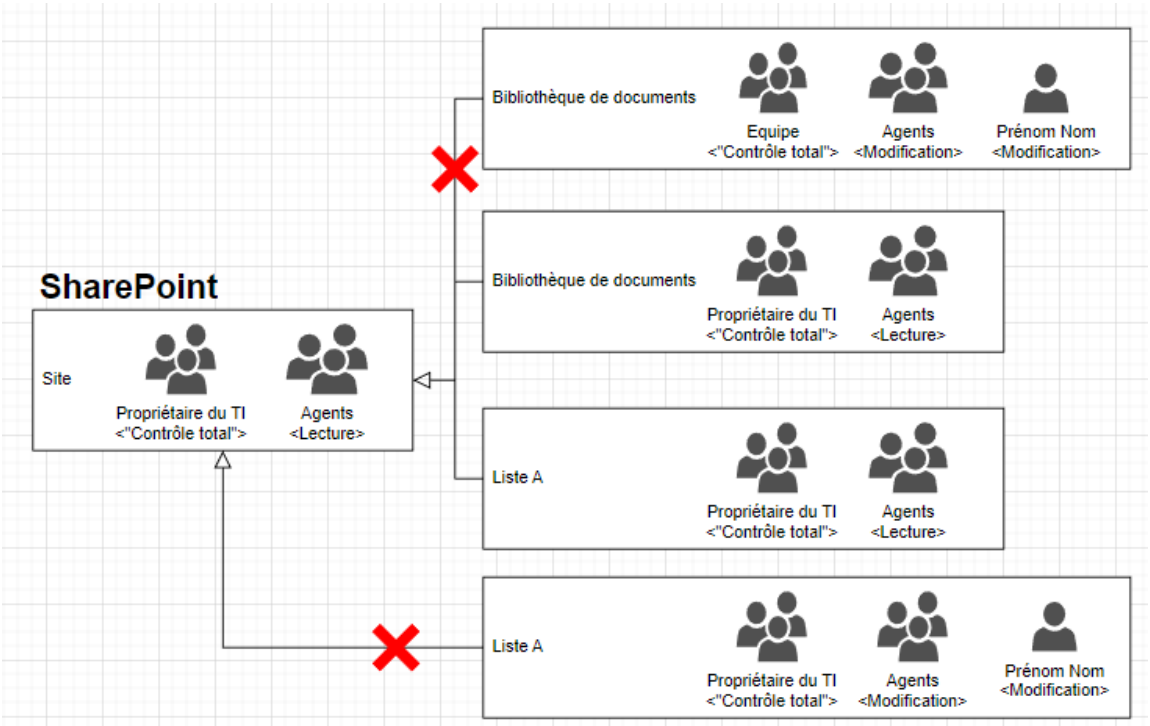

Fig. 6 - Contournement d'héritage des autorisations sur un site SharePoint

Pour résumer, un membre sans droit particulier (tous les agents de l'établissement sauf les « propriétaires ») est, en tant que membre du groupe Microsoft 365 de l'établissement, simple

lecteur du contenu du site, sauf si un propriétaire accorde à ce membre une autorisation supérieure sur un élément, que ce soit directement à lui ou bien à un groupe auquel il appartient.

4. Applications Microsoft Power Apps

Les applications Microsoft Power Apps, qui font partie de la suite Power Platform avec Power BI et Power Automate, sont entièrement distinctes du site SharePoint.

Au niveau national, tout agent a théoriquement la possibilité de créer son application Power Apps. Tout utilisateur Office 365 de SNCF dispose donc d'une licence basique lui permettant de développer en low-code. Il lui faut cependant un environnement Power Apps, qui est mis à disposition à un niveau supérieur à l'établissement.

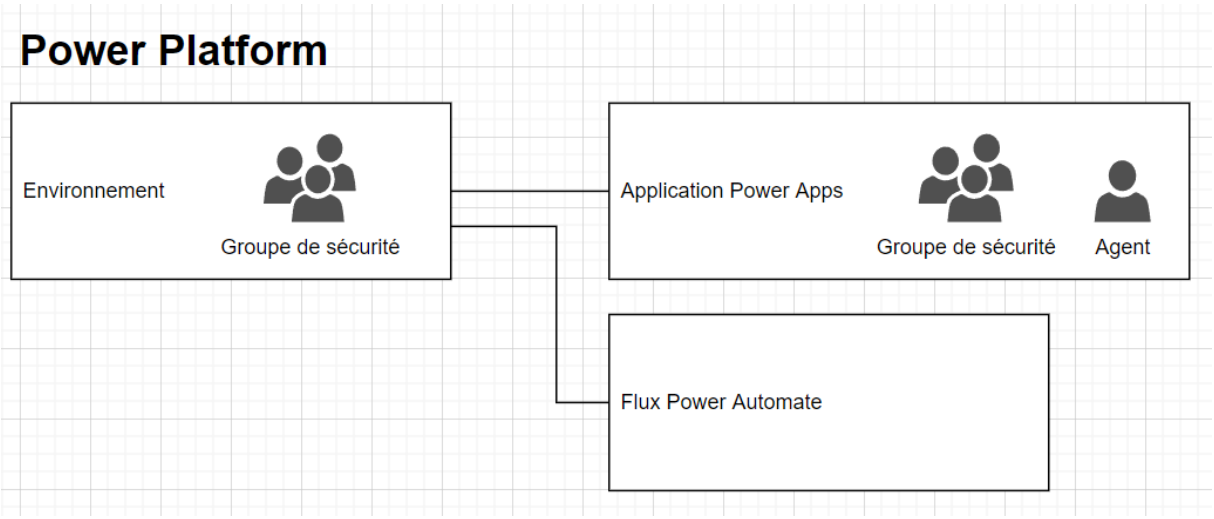

Fig. 7 – Schéma des autorisations Power Platform

Cet environnement est associé à un groupe de sécurité, géré au niveau national, sur lequel nous avons très peu de visibilité. Le fait d'appartenir à ce groupe de sécurité nous permet en tout cas de voir la liste de toutes les applications créées dans l'environnement, y compris celles conçues par un collègue d'un autre établissement. Cependant, il faut disposer d'une autorisation pour pouvoir lancer une application.

Sur la figure 7, on voit que des autorisations sur des applications Power Apps peuvent être données à des groupes de sécurité. Mais au niveau des développeurs de l'établissement, nous n'avons pas la possibilité d'ajouter un groupe de sécurité librement. Par conséquent, il est impossible de donner des droits sur une application à un groupe d'agents, et les autorisations sont données individuellement.

En tant que simple alternante mais employée SNCF, j'ai le droit de créer une application Power Apps (voir mon *compte-rendu sur l'application Power Apps « Achats »*). Pour Microsoft, je suis donc propriétaire de l'application : lorsqu'un agent souhaite accéder à l'application (via un lien obtenu par un collègue), il doit en faire la demande. Le propriétaire doit ensuite ajouter l'agent (figure 9).

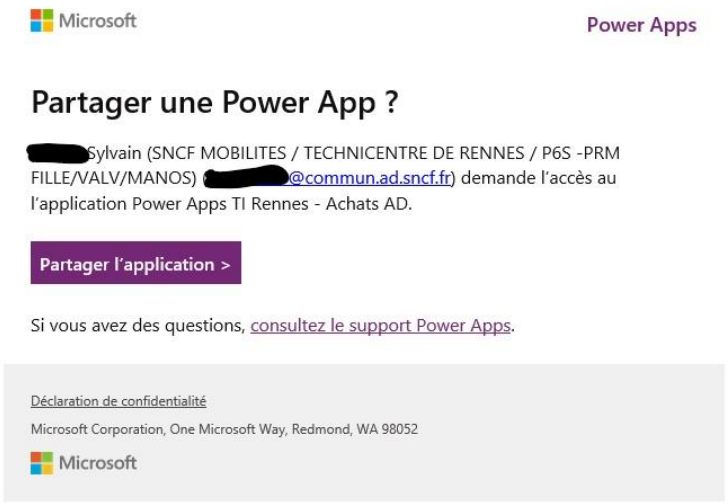

Fig. 8 - Demande d'accès à une application Power Apps envoyée à son propriétaire

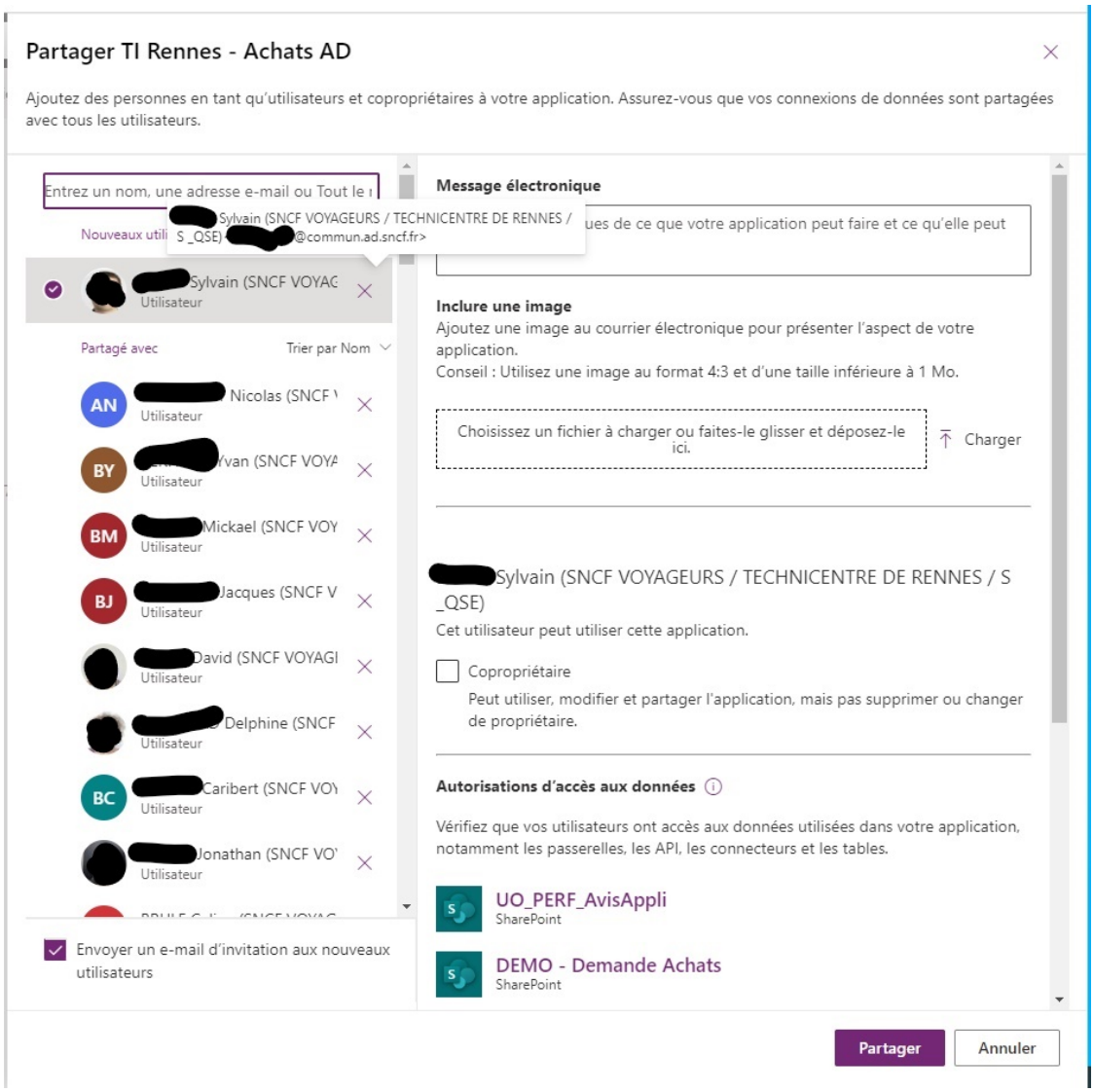

Fig. 9 - Écran de partage d'une application à un agent

On trouve sur cet écran un message d'avertissement intéressant : la section Autorisations d'accès aux données. En effet, pour pouvoir utiliser l'application, les utilisateurs doivent pouvoir accéder à ses sources de données.

5. Power Apps et listes SharePoint

Ce qu'on a vu jusqu'ici permet déjà de voir que Power Apps et listes SharePoint ne sont pas sur le même plan. Un utilisateur peut avoir accès à une application mais ne pas avoir accès à ses sources de données. Or, si n'importe qui peut créer son application, il faut des privilèges particuliers pour pouvoir donner accès à des listes SharePoint.

On peut schématiser l'utilisation d'une application Power Apps par la figure suivante.

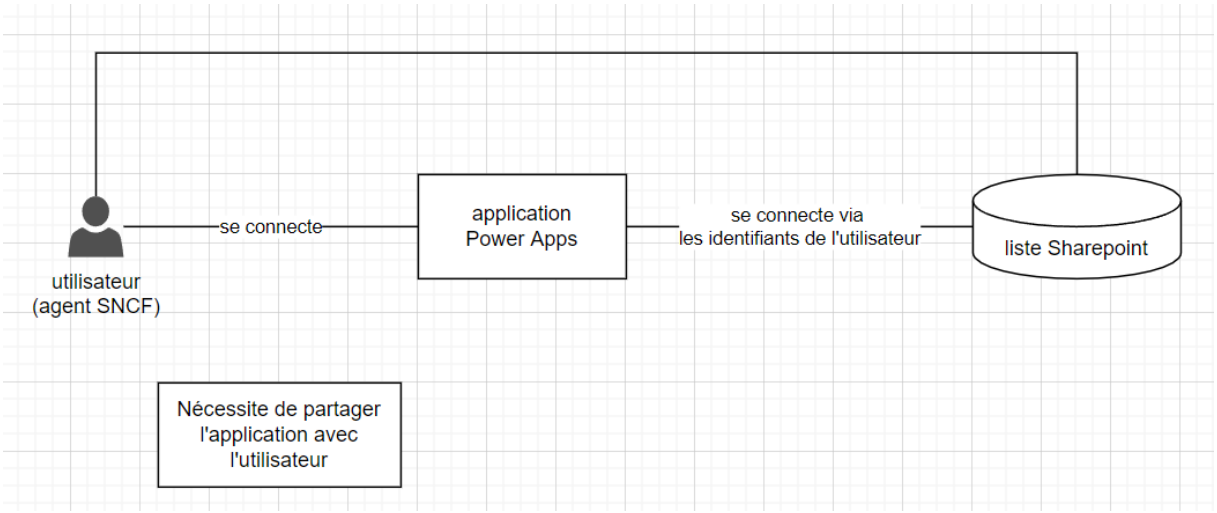

Fig. 10 - Schéma du lien entre application Power Apps et liste SharePoint

Entre Power Apps et ses sources de données, on trouve des connecteurs. Assimilés à des API, ils permettent à l'application de se connecter avec les identifiants de l'utilisateur. Le connecteur vérifie les autorisations que possède l'utilisateur sur une source de données, et récupère/modifie les informations si l'utilisateur en a l'autorisation.

Cette structure a une conséquence : pour pouvoir ajouter une ligne à une liste Power Apps via le formulaire présent dans une application, l'utilisateur doit avoir un droit de modification sur la liste SharePoint. Or, rien ne l'empêche d'accéder à celle-ci via le site SharePoint. Autrement dit, l'utilisateur peut d'une part consulter toutes les lignes de la liste en intégralité, même ce qui ne le concerne pas, et d'autre part modifier une ligne qu'il n'a pas créée.

Quelques garde-fous existent contre la modification abusive (intentionnelle ou accidentelle), car le système effectue des sauvegardes régulières des données. Cependant, rien ne permet de restreindre l'affichage des données.

Une solution envisagée est d'utiliser une base de données Microsoft Dataverse, qui permet une meilleure gestion de la sécurité, et est par ailleurs plus efficace.

6. Microsoft Dataverse

Microsoft Dataverse est un système de gestion de bases de données de Microsoft similaire aux SGBD classiques, qui permet une gestion précise des droits, et interdit à l'utilisateur lambda d'accéder aux données en dehors d'une application.

La mise en place d'applications basées sur Dataverse nécessite une demande aux administrateurs au niveau national, demande qui a été faite pour notre établissement pendant ma période d'alternance. Trois nouveaux environnements nous ont été fournis : développement, recette et production. En mai 2023, la prise en main de Dataverse se fait petit à petit. Elle nécessite notamment de mettre en place de nouveaux groupes de sécurité, puis de migrer les applications existantes de l'ancien environnement vers les nouveaux. Les listes SharePoint devront aussi être transférées, et tout cela nécessite de la réflexion et du temps.

Bien que la question sorte un peu du cadre de cette synthèse, il me paraît utile de préciser que les changements induits par le passage à Microsoft Dataverse n'affecteront pas uniquement les développeurs. Si son utilisation signifie à terme plus de sécurité et une plus grande efficacité, elle signifie aussi pour les utilisateurs moins de libertés mais plus de fiabilité.