Binôme :

- Raphaël Mourtzanakis
- Kévin Canaj

1.

Différents types d'attaques d'un système d'information			
Nom des menaces	**Impacts**	**Description**	**Lien avec l'entreprise**
(D)DoS	Envoie, collecte et lecture des données rendues indisponibles.	Consiste à envoyer plein de requêtes d'une ou plusieurs « personnes » jusqu'à ce que les serveurs crash.	Perte du service du système informatique, serveurs en maintenance, plus possible d'envoyer et collecter des données.
Piratage	L'accès d'un compte administrateur dans le réseau informatique d'une personne externe de l'entreprise et aurait tous les droits.	Une personne externe tente de récupérer notre mot de passe de manières différentes pour se connecter à notre compte.	Une personne pirate la session d'un employer pour récupérer/supprimer des données et même les donner à une entreprise tierce concurrente pour faire couler l'entreprise.
L'Homme du milieu	Les données pendant un transfère sont interceptées et collectées par une personne externe.	Intercepte les données pendant leur transfère entre 2 ou plusieurs individus.	Un concurrent de l'entreprise écoute la conversation entre deux employés ou, pendant un envoie de formulaire par un utilisateur avec des réponses en rapport avec des données personnelles pouvant être lues.

Fraude	Faux collègue ou technicien qui nous demande des informations pour les voler ou fait installer des logiciels malveillants.	Se fait passer pour une autre personne afin de contacter une personne de l'entreprise en demandant des informations en croyant que c'est une personne de confiance.	Un faux technicien contact un employer et fait télécharger un virus que l'employer naïf télécharge et se fait infecter avec le reste du réseau informatique.
Virus	S'infecte dans les serveurs et les données sont collectées par un inconnu, données supprimées.	Un programme qui exécute des tâches afin de collecter, supprimer, modifier des données sur l'ordinateur en question.	Logiciel malveillant dans la session des employés pour collecter/supprimer les données de l'entreprise et accéder au réseau informatique.
Vol de mot de passe	Peut être vu par une personne pour l'utiliser afin de se connecter à notre compte.	Une personne externe qui nous regarde écrire notre mot de passe pour l'utiliser, ou une personne qui utilise notre mot de passe qu'on a noté quelque part.	Un employé qui laisse son mot de passe noté quelque part ou on la vu l'écrire, et quelqu'un se fait passer pour lui et par exemple supprimer des données sans faire exprès et on ne peut pas savoir qui l'a vraiment fait.
Rançonlogiciel	Impossible d'accéder aux données sans devoir payer (pas garanti de retrouver les données en payant).	Logiciel malveillant qui bloque nos données pour nous demander de l'argent en échanges de les rendre accessibles de nouveau.	Perte d'accès aux données et l'entreprise ne peut plus faire de profits et pertes d'utilisateurs, perte d'argent en payant la rançon.

Erreur des ressources humaines	Modifer/Supprimer sans faire exprès des données, laisser sa session ouverte.	Un employer sur son compte qui modifie/supprime des données sans faire exprès, ou un autre collègue qui utilise le compte de son collègue pour faire des choses.	Grande perte de données dans l'entreprise, doit sensibiliser les employés, perte de profits. Perte de données d'un employé, ou d'utilisateurs.
Évènement naturel	Dégâts physiques sur les serveurs et possibilité de pertes.	Catastrophes naturelles comme un incendies, séismes, inondations, etc. qui endommagent les serveurs avec les données.	Il y a une catastrophe naturelle, le matériel est abîmé, les employés ne peuvent plus revenir au travail pendant un moment, perte d'argent.

2.

Précautions et méthodes de protections		
Nom des menaces	**Précautions**	**Méthodes de protections**
(D)DoS	Bloquer l'accès au surplus de données et l'accès aux bots.	Avoir des serveurs de secours pour avoir moins de problème au fait de ne pas avoir accès aux serveurs.
Piratage	Utiliser des mots de passe forts et utiliser la double authentification.	Changer régulièrement de mot de passe et bloquer notre compte si on s'en aperçoit et bloquer le compte de ceux qui ont été piratés pour ne pas qu'ils nous envoient de mails de fraude par exemple.
L'Homme du milieu	Utiliser des clés chiffrés.	Chiffrer les conversations pour éviter que les messages interceptés soient lus.