|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Partie prenante | Chemins d’attaque | Mesures de sécurité | Menace initiale | Menace résiduelle |
| Secrétaire | Vengeur qui arrête de la prise de rdv par compromission (via une clé USB piégée, phishing) du pc de la secrétaire | Blocage des ports USB.  Formation du personnel aux risques cyber. | 4 | 1 |
| Secrétaire | Le crime organisé et/ou concurrent offrent un pot de vin ou menacent pour accéder aux info de contact des patients | Avantages extra-légaux.  Clause contractuelle de non divulgation. | 4 | 1 |
| Secrétaire | Pièce jointe piégée par l’envoi de mail frauduleux ou clé USB piégée pour atteindre les données de contact des clients. | Blocage des ports USB.  Formation du personnel aux risques cyber. | 4 | 1 |
| Plateforme en ligne | Arrêt de l’activité générale dû à une coupure d’internet volontaire | Avoir une seconde ligne internet (redondance des câbles, boitier 4G). | 1 | 0.75 |
| Médecin | Pièce jointe piégée par l’envoi de mail frauduleux ou clé USB piégée pour obtenir les identifiants du médecin | Installation d’une solution de sécurité (AV).  Formation du personnel aux risques cyber. | 3 | 0.89 |
| Médecin | Utilisation des identifiants du médecin ou d’une sessions ouverte pour voler des données des dossiers médicaux | Forcer le médecin à changer de mdp régulièrement.  Double authentification.  Monitoring des accès. | 3 | 0.89 |