

**Exemple d'analyse de risque : base de données accessible uniquement à une collaboration en chimie. Cette collaboration regroupe plusieurs chercheurs d'unités et de pays différents.**

Les données ont des besoins de:

- **Confidentialité et intégrité très importants** car elles peuvent donner lieu à un dépôt de brevet avec un laboratoire pharmaceutique.
- **Disponibilité moyenne** car toute la collaboration (plusieurs labos à l'étranger) doit y accéder, mais on peut tolérer une demi-journée d'interruption sans problème.

Les données peuvent être sur :

- Le **serveur** qui les héberge normalement
- Le **poste de travail** du chercheur qui soit a fait des extractions de la base, soit élabore les données qui vont alimenter la base.

Elles peuvent être accédées depuis n'importe quel poste de travail en dehors du laboratoire sans chiffrement mais avec une authentification par login et mot de passe.

### **1. Le serveur**

- Il n'est pas redondé mais installé sur une machine virtuelle que l'on sait (il existe des documents, des procédures qui décrivent comment faire) cloner ou réinstaller en une demi-journée sans problème.
- La base de données est normalement sauvegardée régulièrement mais on n'a jamais fait de restauration de zéro de la base de données depuis l'installation de la machine.
- Il est installé dans une salle machine avec une climatisation qui est gérée par l'université et dont on ne sait pas grand-chose (contrat de maintenance ?).
- La salle machine possède un système de contrôle d'accès (clef, badge,...) qui ne permet l'accès qu'aux personnes autorisées. Mais on ne sait pas très bien qui a accès à cette salle en dehors du service informatique (gardien, ménages,...)
- L'alimentation électrique de la salle machine est récente et possède un onduleur qui permet d'arrêter correctement la machine en cas de coupure (et si quelqu'un est présent).
- Le serveur hôte n'est pas en RAID.
- L'unité est hébergée par l'université. Le réseau est entièrement géré par le CRI de l'université.
- Les logs du serveur ne sont pas conservés.

### **2. Les postes de travail**

- Authentification dans le laboratoire via un AD
- Le chercheur utilise un compte administrateur local pour travailler
- Pas de chiffrement.
- Les données sont recopiées localement sur les disques.
- Pas de mécanisme automatique de sauvegarde des disques locaux
- Les locaux sont facilement accessibles à tous sans contrôle d'accès

### **3. Scénario 1 :**

Suite à **une panne de climatisation** le serveur hôte est en panne, toutes les VMs sont indisponibles. Une nouvelle VM est installée à partir du clone, il faut réinstaller la base de

données, la dernière sauvegarde correcte de la base remonte à plusieurs mois et la réinstallation de la base depuis une sauvegarde n'a jamais été faite...

**4. Scénario 2 :**

Un chercheur ayant les droits d'administration sur son poste a mis ses disques locaux en partage sans protection au monde entier. Les données confidentielles sont accessibles à tous et sont récupérées depuis ses partages par un visiteur mal intentionné.

**5. Scénario 3 :**

Un chercheur utilise son portable personnel pour accéder à la base de données depuis un cybercafé. Les accès à la base sont non chiffrés. Son compte est récupéré depuis le cybercafé. Une personne mal intentionnée se connecte au serveur et détruit des données par jeu. Pas de log des accès au serveur, on ne s'aperçoit pas du problème avant plusieurs semaines.

**6. Scénario 4 :**

Une personne mal intentionnée rentre dans la salle machine et arrête ou détruit le serveur.

**7. Scénario 5 :**

Vol de l'ordinateur portable du chercheur. Il n'est pas chiffré et contient des données de la collaboration avant dépôt de brevet.