**Security – technical considerations - Sécurité - considérations techniques**

High Level:

- ensure that there is a documented set of technical ontrols mandated

- ensure that there is audit process against those controls

Haut niveau:

- s’assurer qu’il existe un ensemble documenté d’outils techniques obligatoires

- S'assurer qu'il existe un processus d'audit contre ces contrôles

Many government audit processes assume a microsoft environment. You might need to do additional work to ensure linux machines and applications are adequately covered.

De nombreux processus d'audit gouvernementaux supposent un environnement Microsoft. Vous devrez peut-être effectuer des tâches supplémentaires pour vous assurer que les machines et applications Linux sont correctement couvertes.

Example controls are in resources directory. They can be taken and customised.

TopTen for rapid assessment

1. Operating system is a LTS (long term service edition)
2. There is an automatic process for applying OS security patches
3. Host based firewall configured allowing minimal access
4. Access is via ssh according to agreed policy - keys, no root access etc
5. DHIS2 version is not more than 3 versions behind latest release. Process exists to apply patch releases regularly.
6. Automated backup system is in place and regularly tested, including offsite.
7. Postgresql database accesss controls allow minimal access
8. Web-proxy server is properly (ssllabs test A+) configured with SSL
9. Database data is on separate data partition (allowing encryption at rest, performance settings)
10. Monitoring and alerting system is in place (wide range of options depending on environment. eg. boombox might be fine with email + logwatch + munin )

Every system must have a documented data owner and responsible administrator!!

Les contrôles exemple sont dans le répertoire des ressources. Ils peuvent être pris et personnalisés.

TopTen pour une évaluation rapide

1. Le système d'exploitation est un LTS (édition de service à long terme)

2. Il existe un processus automatique pour appliquer les correctifs de sécurité du système d'exploitation

3. Un pare-feu basé sur l'hôte configuré pour un accès minimal

4. L'accès se fait via ssh selon la politique convenue - clés, pas d'accès root, etc.

5. La version DHIS2 n'est pas plus de 3 versions derrière la dernière version. Le processus existe pour appliquer régulièrement des versions de patch.

6. Un système de sauvegarde automatisé est en place et régulièrement testé, y compris hors site.

7. Les contrôles d'accès aux bases de données postgresql permettent un accès minimal

8. Le serveur Web-proxy est correctement configuré (test ssllabs A +) configuré avec SSL

9. Les données de la base de données se trouvent sur une partition de données distincte (permettant le cryptage au repos, paramètres de performance)

10. Le système de surveillance et d'alerte est en place (une large gamme d'options dépend de l'environnement. Par exemple, boombox peut convenir avec le courrier électronique + logwatch + munin)

Chaque système doit avoir un propriétaire de données documentaires et un administrateur responsable !!