

Audit de Sécurité

Sujet 3

FUTURZO



Les réseaux du futur

- Faut-il faire une main courante différente du 1er sujet ou doit-on tout mettre dans la même?

Tout noter, pour le fonctionnement interne

- Est ce qu'il existe déjà des solutions de sécurisation?

Juste AV => BitDefender

- De quel budget disposons-nous?

Limité => nous sommes pauvres

1) Laboratoire :

- De quelle envergure sera le laboratoire? (Combien de postes clients)

4-5 postes

- Ce projet ne se fait-il qu'avec le matériel fourni en salle Z020?

Oui

2) Proposition de solutions :

2.1) Protection proactive :

Liste non-exhaustive :

-un WSUS ?

Oui

-Sensibilisation des utilisateurs?

Oui – charte RGPD

-Des stations blanches?

À faire

-Une vérification des mises à jours systèmes hebdomadaires obligatoires?

Oui, programmé

-Un scan obligatoire pour toutes les machines étrangères à la mairie?

Selon nous...

-Des bloqueurs pour les ports USB/RJ45?

oui

-Mise en place d'une équipe d'intervention "CYBER"?

Non => admins réseaux

-Séance de "test" d'incidents pour améliorer la relation entre les techniciens et les utilisateurs?

Oui

-Un durcissement des équipements physiques?

Oui

2.2) Protection :

Mise en place :

-Un proxy avec liste blanche ou noir?

Oui

-Un ou des IDS et IPS?

Oui, mais pas de matériel

-Une zone dématérialisée?

Non

-Un accès distant SSH ou telnet?

Oui, depuis internet (sous-entendu VPN)

-Une restriction d'interface administrateur depuis internet?

Oui

exemple) -Limiter l'accès physique au poste? (système de badge par

Oui

-Un système de sauvegardes?

Oui

-Quel type de PRA utilise t-on? (onduleur par exemple)

Oui, à nous de choisir

-Une journalisation des évènements/incidents?

Oui

3) Sauvegarde :

Mise en place :

-Un Cloud?

Non

-Un NAS?

SYNOLOGY

-Un lecteur de bande externe?

Non

-Une sauvegarde des données du serveur ?

Environ 250Go de données à sauvegarder.

-Compleète/Journalière/Incrémentielle ?

A nous de voir

-A quelle fréquence?

A nous de voir