PROJET 1

POUPOT Elliot
SIO SISR 2023-2025

Contexte :

Le cabinet **Horizon Management**, spécialisé dans le **conseil financier**, souhaite moderniser et sécuriser son infrastructure informatique afin de **protéger efficacement ses données sensibles**.
Conscients des **risques liés à la cybersécurité**, les associés cherchent à se prémunir contre les **cyberattaques, pertes de données** et **accès non autorisés**. Ils expriment également le besoin d'un **système de sauvegarde fiable** et d'une **accessibilité fluide** aux informations, depuis le bureau comme à distance, sur PC comme sur mobile.

Enfin, le cabinet souhaite **structurer l'usage de son système informatique**, en établissant des **règles claires et un cadre sécurisé**, mais manque de repères pour le mettre en place. Une **approche globale**, intégrant **protection, accessibilité et encadrement**, est donc attendue.

Objectifs :

Objectifs généraux

- Sécuriser les données sensibles contre les cyberattaques et les accès non autorisés.
- Garantir l'**accessibilité** des informations à distance et en mobilité.
- Mettre en place une **sauvegarde fiable** et récurrente pour éviter toute perte de données critiques.
- Structurer l'usage informatique du cabinet en définissant des **règles d'utilisation** claires et efficaces.

Objectifs techniques

- Implémenter une **architecture réseau sécurisée** avec pare-feu Pfsense et segmentation.
- Mettre en place un **accès distant sécurisé** via VPN et authentification multi-facteurs.
- Déployer une **solution de sauvegarde automatisée** locale et cloud (Nextcloud).
- Installer des outils de **supervision et monitoring** pour prévenir les incidents.
- Définir une **politique informatique** incluant des règles, des restrictions et des bonnes pratiques.

Périmètres :

Périmètre fonctionnel

Ce projet couvre la **sécurisation, la gestion, la sauvegarde et l'accessibilité** des données et ressources numériques du cabinet Horizon Management.

Fonctionnalités principales

Infrastructure réseau

- Mise en place d'un **pare-feu Pfsense** pour sécuriser les flux réseau (voir **Annexe 1** – Schéma réseau).
- Déploiement ou renouvellement de l'**antivirus CrowdStrike** sur **10 postes**.
- Installation d'un **serveur AD DS (Active Directory Domain Services)** :
    - Gestion centralisée des utilisateurs et des authentifications.
    - Stockage et **partage des fichiers** via un serveur dédié.
- Déploiement de **Mailinblack** pour sécuriser la messagerie contre le **phishing, le spam et les malwares**.

Sauvegarde et stockage

- Mise en place d'un **serveur de sauvegarde** intégrant :
    - **Nextcloud** pour la synchronisation et l'accès aux fichiers.
    - Un **script de sauvegarde automatisé**.
- Politique de sauvegarde :
    - **Sauvegarde complète** chaque **dimanche**.
    - **Sauvegardes incrémentales** du **lundi au samedi**.

Accès distant et mobilité

    - Installation d'un **VPN OpenVPN** pour les connexions distantes sécurisées depuis PC ou mobile.
- Création d'un **réseau Wi-Fi invité isolé**, distinct des ressources internes.

Formation et sensibilisation

- Organisation de **stages de sensibilisation à la cybersécurité**.
- Formation des collaborateurs à l'usage des nouveaux outils (VPN, stockage, AD DS…).

Plan de mise en oeuvre :

1. Installation et configuration Windows Serveur 2022

La première étape consiste à installer **Windows Server 2022** sur le serveur physique ou virtuel.

Voici ce que cela inclut :

- **Installation de l'OS :** Utilisation d'un média d'installation (DVD, USB, ou image ISO) pour installer Windows Server 2022 sur le matériel.
- **Configuration de base :** Après l'installation, il faudra configurer des paramètres de base comme l'activation de Windows, les paramètres régionaux, et l'activation du serveur pour en faire un contrôleur de domaine.
- **Mise à jour :** Installation des dernières mises à jour et correctifs pour garantir la sécurité et la stabilité du serveur.
- **Activation et licence :** S'assurer que la licence du serveur est activée correctement.

2. Installation du service AD DS

Active Directory Domain Services (AD DS) est essentiel pour gérer un réseau d'entreprise. Il permet d'authentifier les utilisateurs et de gérer les ressources du réseau.

Voici les étapes :

- Installation d'AD DS : Utilisation de l'outil Gestionnaire de serveur pour installer le rôle Active Directory Domain Services.
- Promotion du serveur en contrôleur de domaine : Une fois AD DS installé, il faudra promouvoir le serveur en contrôleur de domaine en le rejoignant à un nouveau domaine (ou en le rejoignant à un domaine existant).
- Création du domaine : Si c'est la première fois, un nouveau domaine (par exemple, "mondomaine.local") sera créé.
- Configuration des utilisateurs et groupes : Une fois le contrôleur de domaine configuré, tu pourras gérer les utilisateurs, groupes et objets de l'Active Directory.

3. Installation et configuration du service DHCP

Le service **DHCP** permet de distribuer automatiquement des adresses IP aux ordinateurs et autres appareils connectés au réseau, ce qui simplifie la gestion des adresses IP.

Voici comment procéder :

- **Installation du rôle DHCP :** Le rôle **DHCP** est ajouté via le **Gestionnaire de serveur**.
- **Configuration de la plage d'adresses IP :** Après l'installation, il faudra configurer une plage d'adresses IP que le serveur DHCP attribuera aux clients.
- **Définir les options DHCP :** Cela inclut la configuration des **serveurs DNS**, de la **passerelle par défaut** et d'autres paramètres réseau nécessaires.
- **Activation du service :** Enfin, le service DHCP doit être activé pour qu'il puisse commencer à attribuer des adresses IP aux périphériques du réseau.

4. Installation du service de DNS

Le service **DNS** est crucial pour la résolution des noms de domaine dans le réseau local, facilitant ainsi la communication entre les serveurs et les clients.

Voici ce qui doit être fait :

- **Installation du rôle DNS :** Le rôle **DNS** est installé via le **Gestionnaire de serveur**, si ce n'est pas déjà fait lors de l'installation d'AD DS.
- **Configuration des zones DNS :** Une zone **DNS primaire** pour le domaine sera créée (par exemple, "mondomaine.local"). Cela permet de traduire les noms de domaine en adresses IP.
- **Enregistrement des ressources DNS :** Les enregistrements de ressources, comme les **enregistrements A** pour les hôtes et les **enregistrements MX** pour la messagerie, devront être configurés.
- **Configuration de la réplication DNS** : Si le réseau contient plusieurs serveurs DNS, la réplication entre les serveurs doit être configurée pour garantir la continuité des services.

5. Création du partage de fichiers interne par GPO

Un **partage de fichiers interne** permet de centraliser l'accès aux documents et ressources sur le réseau. Utiliser les **Group Policy Objects (GPOs)** pour le gérer offre un contrôle centralisé sur les permissions d'accès.

Voici les étapes :

- **Création du dossier partagé :** Sur le serveur, créer un dossier destiné à être partagé.
- **Définition des permissions :** Configurer les **permissions NTFS** sur le dossier pour déterminer qui peut y accéder et ce qu'ils peuvent y faire (lecture, écriture, suppression, etc.).
- **Création de la GPO** : Une **GPO** est créée pour définir la stratégie de partage et l'appliquer à une unité organisationnelle (OU) spécifique. Cela peut inclure la configuration du partage de fichiers pour un groupe d'utilisateurs ou d'ordinateurs.
- **Attribution de la GPO :** Une fois la GPO configurée, elle est liée à l'unité organisationnelle (OU) contenant les utilisateurs ou groupes de sécurité qui auront accès au partage.
- **Application et vérification :** Enfin, la **GPO** doit être mise à jour sur les postes de travail clients pour que les utilisateurs puissent accéder au partage de fichiers en toute transparence.

6. Mise en place d’une solution RAID 5.

Vue d’ensemble

- **Type** : RAID 5 (parité répartie, tolérance à une panne disque).
- **Nombre minimum de disques** : 3 disques durs.
- **Tolérance de panne** : 1 disque dur peut tomber sans perte de données.
- **Performance** :
    - **Lecture** : rapide (lecture parallèle sur plusieurs disques).
    - **Écriture** : plus lente (calcul de parité).
- **Sécurité** : Protection des données grâce à la parité.
- **Reconstruction** : En cas de panne, possibilité de reconstruire le RAID après remplacement du disque.
- **Usage recommandé** : Serveurs de fichiers, bases de données, archivage critique avec accès fréquent.

7. NextCloud sur Debian

Pour répondre aux besoins de **sauvegarde**, de **partage sécurisé** de fichiers et de **travail collaboratif**, la solution **Nextcloud** sera déployée sur une distribution **Debian**.

Cette solution auto-hébergée permet une maîtrise complète des données, avec un accès sécurisé depuis n'importe quel appareil (PC, mobile, tablette), en local comme à distance.

Étapes de mise en œuvre :

- **Installation de Debian**
  Un système Debian est installé sur une machine virtuelle dédiée ou un serveur physique, choisi pour sa **stabilité** et sa **sécurité**. Le système est mis à jour et durci (pare-feu, services minimaux, SSH sécurisé).
- **Déploiement de Nextcloud**
  Nextcloud est installé manuellement ou via un conteneur (ex. Docker) pour plus de flexibilité. Un **serveur web Apache ou Nginx**, une **base de données MariaDB** et **PHP** sont configurés en amont.
- **Configuration SSL et sécurité**
  Le serveur est sécurisé avec un **certificat SSL/TLS** (Let's Encrypt par exemple) afin de garantir le chiffrement des échanges. Des restrictions IP et une authentification forte sont ajoutées.
- **Création des comptes utilisateurs**
  Des comptes sont créés manuellement ou via une synchronisation LDAP avec l'Active Directory pour permettre une connexion centralisée avec les mêmes identifiants.
- **Définition du plan de sauvegarde**
  Nextcloud est couplé à un **script de sauvegarde automatisée** (quotidienne et hebdomadaire) pour garantir la restauration rapide des fichiers en cas d'incident.

8. OpenVPN

Afin de permettre aux collaborateurs de se connecter de manière **sécurisée au réseau interne à distance**, le service **OpenVPN** sera mis en place. Il garantit un **canal chiffré** entre l'utilisateur distant et l'infrastructure de l'entreprise.

Étapes de mise en œuvre :

- **Installation du serveur OpenVPN**
  Le serveur OpenVPN est déployé sur un hôte dédié (physique ou virtuel) sous Linux (Debian recommandé), avec une **configuration en mode routé (tun)** pour assurer l'isolement du trafic.
- **Création des certificats**

Phase	Description	Durée estimée
Phase 1	Audit, définition des besoins, planification	1 semaine
Phase 2	Installation et configuration des équipements (AD, PfSense, sauvegarde)	2 semaines
Phase 3	Mise en place des accès sécurisés (VPN, Mailinblack), tests et validation	1 semaine
Phase 4	Formation des utilisateurs, documentation, mise en production	1 semaine
Total estimé		**5 semaines**

  Une **autorité de certification (CA)** est générée pour créer les certificats serveur et clients. Cela permet une **authentification forte** à deux facteurs : certificat + mot de passe.
- **Configuration du pare-feu (Pfsense)**
  Le pare-feu est configuré pour autoriser le trafic VPN sur le port choisi (par défaut UDP 1194), et rediriger les connexions entrantes vers le serveur VPN.
- **Déploiement des profils clients**
  Chaque collaborateur reçoit un **fichier de configuration OpenVPN** personnalisé (.ovpn) avec son certificat. Des clients OpenVPN sont installés sur PC et mobiles.
- **Tests de connexion et contrôle d'accès**
  Des tests sont effectués pour garantir la bonne connexion des utilisateurs à distance. L'accès aux ressources internes est restreint selon les droits définis dans l'Active Directory.

Contraintes techniques :

Utilisation de **PfSense** comme pare-feu principal.

- Déploiement d'un **serveur Windows Server** pour AD DS et stockage.
- Infrastructure compatible avec des **postes sous Windows 11** et mobiles Android/iOS.
- Solutions de sécurité et sauvegarde choisies pour leur **conformité RGPD** et leur **fiabilité**.
- Infrastructure installée **sur site**, avec **accès distant** sécurisé uniquement via VPN.

Estimation des délais et coûts :

L'ensemble du projet s'étale sur plusieurs semaines en raison des différentes étapes de configuration, de validation et de mise en production. Voici un détail des étapes, incluant le temps nécessaire pour obtenir les autorisations du RSI.

Poste	Détail	Coût estimé
Main d'œuvre	180 heures à 11€/h	1 980 €
Logiciels	Windows Server, Nextcloud (open source), Mailinblack, CrowdStrike	À estimer
Matériel	Serveur, poste de sauvegarde, routeur, onduleur	À estimer
Formation	Sessions internes	Inclus
Total estimé		**≈ à préciser selon devis matériel + licences**

Phase 1 : Préparation et obtention des accès

Besoin de l'accord et des accès en interne avec la personne régissant la partie informatique.

Phase 2 : Installation et configuration des services (AD DS, DNS) et tests

Durée estimée : 3 semaines

- Installation du serveur Windows Server 2022 et mise en place du rôle de contrôleur de domaine (Active Directory Domain Services).
- Configuration du service DNS pour résoudre les domaines avec leurs IP correspondantes.
- Connectivité effective des équipements réseau
- Configuration des GPO
- Test des fonctionnalitées de tous les services (DHCP, DNS, GPO) ainsi que de la conectivité entre les équipements réseaux (ROUTEUR, SWITCH).
- Installation NextCloud et remote access.
- Installation système de sauvegarde

Dépendance : Mise en production à la suite de la validation du RSI.

Phase 3 : Documentation, formation et suivi de l'infrastructure lors de la mise en production.

Durée estimée : 1 semaine

- Mise en production de l'infrastructure virtualisée et testée.
- Support utilisateur au niveau des documentation ainsi que pour les techniciens
- Suivi de l'infrastructure afin d'intervenir pour les possible ajustements de configuration.

Dépendance : Cette étape dépend entièrement de la phase de test précédemment réalisée.

Délai global : 5 semaines