

# Rapport de stage – 2025/2026



Auteur : Adjou Rayane

Date : 08/09/2025-20/12/2025

Contexte : Stagiaire Ingénieur chez Inter Resto

## **Introduction**

Dans le cadre de ma dernière année d'études en école d'ingénieur informatique, j'ai effectué un stage de cinq mois au sein de l'entreprise INTERRESTO, située à Avelin. Ce stage avait pour objectif de me confronter à un environnement professionnel réel, de mettre en pratique les compétences acquises au cours de ma formation, et de contribuer à des projets concrets à forte valeur ajoutée pour l'entreprise.

Durant cette période, j'ai été amené à travailler sur deux missions principales : la mise en place d'une solution de centralisation des fichiers pour améliorer la collaboration interne, et la réalisation d'un audit de cybersécurité visant à renforcer la sécurité du système d'information. Ces deux projets, bien que distincts, s'inscrivent dans une même logique d'optimisation de l'infrastructure informatique et de sensibilisation aux bonnes pratiques numériques.

Ce rapport présente dans un premier temps l'entreprise d'accueil et son environnement, puis détaille les deux projets réalisés, en mettant en lumière les objectifs, les contraintes rencontrées, les solutions mises en œuvre, ainsi que les perspectives d'évolution. Il se conclut par un bilan personnel et professionnel de cette expérience.

## **Présentation de l'entreprise**

INTERRESTO est une société par actions simplifiée fondée en 2017, dont le siège social est situé à Avelin, dans la région Hauts-de-France. Elle est spécialisée dans le commerce de gros alimentaire à destination des professionnels de la restauration. L'entreprise propose une large gamme de produits frais, surgelés et secs, et s'adresse principalement aux restaurateurs, traiteurs, hôtels et établissements de restauration collective.

Avec un effectif compris entre 20 et 49 salariés, INTERRESTO dispose de plusieurs dépôts logistiques répartis dans la métropole lilloise, notamment à Wasquehal, Lille Sud, Templemars et Avelin. Cette organisation lui permet d'assurer une distribution rapide et efficace sur l'ensemble de la région. L'entreprise se distingue par sa spécialisation sectorielle, sa réactivité logistique et sa capacité à répondre aux besoins spécifiques de ses clients professionnels.

Sur le plan juridique, INTERRESTO est enregistrée sous le SIREN 824 167 274, avec un capital social de 100 000 euros. Elle est rattachée à la convention collective du commerce de détail et de gros à prédominance alimentaire. En 2023, elle a réalisé un chiffre d'affaires estimé à 26,7 millions d'euros, pour un résultat net d'environ 107 million d'euros, ce qui témoigne d'une bonne santé financière et d'une rentabilité maîtrisée.

Durant mon stage, j'ai intégré le service informatique ou j'étais le seul, en lien direct avec les équipes administratives et commerciales. J'ai pu observer une organisation structurée autour de plusieurs services (comptabilité, commercial, marketing, administration), chacun disposant de ses propres outils et méthodes de travail. Cette immersion m'a permis de mieux comprendre les enjeux opérationnels d'une PME dans le secteur agroalimentaire, ainsi que les besoins spécifiques en matière de gestion documentaire, de sécurité des accès et de sensibilisation aux risques numériques.

## Projet de centralisation des fichiers

### Constat initial et objectifs

Lors de mon stage, j'ai été chargé de mettre en place une solution de **centralisation des fichiers** au sein de l'entreprise. Celle-ci compte 16 collaborateurs répartis dans différents services (Comptabilité, Commercial, Marketing, Administration, etc.). Avant ce projet, chacun stockait et gérait ses propres documents, ce qui créait des problèmes de communication, de duplication de fichiers et une perte de temps considérable. L'objectif a donc été de proposer une organisation commune, sécurisée et simple d'utilisation, tout en tenant compte des contraintes techniques et financières de l'entreprise.

## Contraintes techniques et choix de la solution

Après analyse, les besoins principaux concernaient la création d'un espace partagé accessible à tous, la mise en place de dossiers réservés à chaque service afin de garantir la confidentialité, et la nécessité de trouver une solution économique. En effet, l'entreprise ne souhaitait pas souscrire à des abonnements cloud (OneDrive ou SharePoint) et ne disposait pas de licence Windows Server. De plus, le serveur en place ne contenait qu'un seul disque dur de 1 To hébergeant également le système, ce qui représentait une contrainte supplémentaire à prendre en considération.

Face à ces limites, j'ai choisi de mettre en place une solution reposant sur un **groupe de travail (Workgroup)**, adaptée à une structure de petite taille et suffisante pour gérer les 16 collaborateurs.

## Conception de l'arborescence

J'ai d'abord conçu une **arborescence de dossiers** claire et hiérarchisée : un dossier principal nommé *Commun* accessible à l'ensemble des employés, ainsi que des sous-dossiers pour chaque service, avec un accès restreint aux seuls membres concernés (*voir figure 1*). Cette organisation permet d'allier partage et confidentialité.

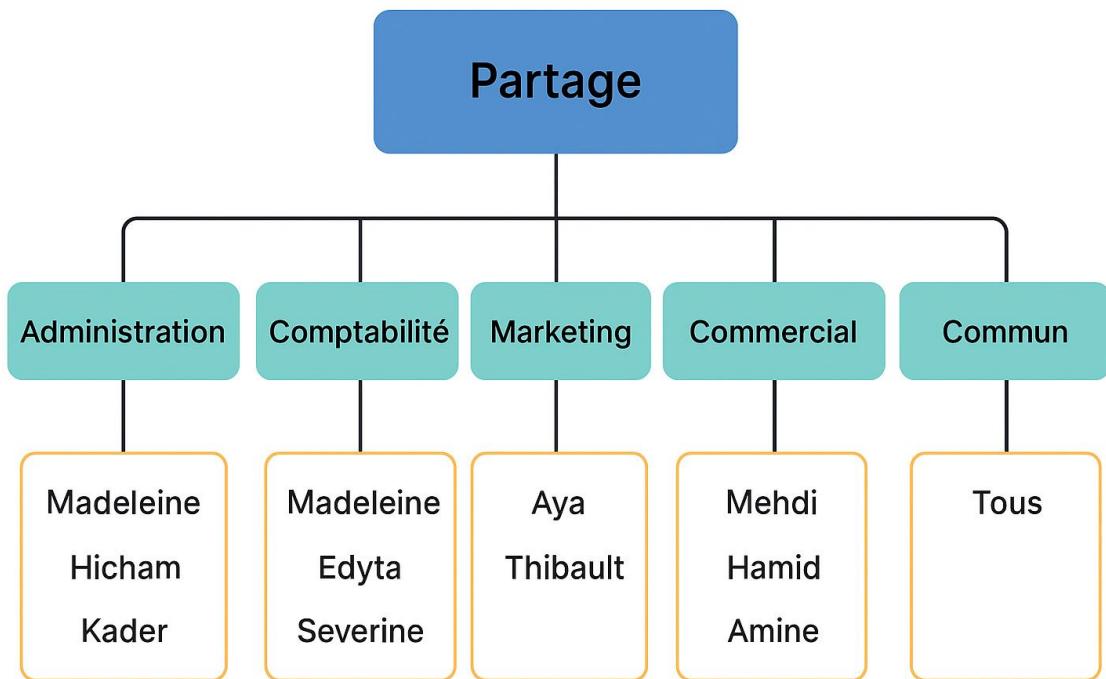


Figure 1 : Schéma de l’arborescence des dossiers.

## Création des utilisateurs et des groupes

Afin de gérer efficacement les accès, j'ai créé des **utilisateurs locaux pour chaque collaborateur** ainsi que des **groupes correspondant aux services** (Comptabilité, Marketing, Commercial, etc.). Chaque utilisateur a été intégré à son groupe, ce qui m'a permis d'appliquer les permissions non pas individuellement mais directement au niveau des groupes (*voir figure 2 et 3*). Cette méthode simplifie la gestion et permet d'évoluer facilement si de nouveaux employés rejoignent l'entreprise.

Iusrmgr - [Utilisateurs et groupes locaux (local)\Utilisateurs]

Fichier Action Affichage ?

Utilisateurs et groupes locaux (local)

- Utilisateurs
- Groupes

Nom	Nom complet	Description	Actions
Administrateur...		Compte d'utilisateur administrateur	Utilisateurs
Amine	Amine		
Avelin			
Aya	Aya		
DefaultAcco...		Compte utilisateur géré par l'administrateur système	
Edyta	Edyta		
Hamid	Hamid		
Hicham	Hicham		
Invité		Compte d'utilisateur invité	
Kader	Kader		
Madeleine	Madeleine		
Mehdi	Mehdi		
Miloud	Miloud		
PStage	Stage		
Severine	Severine		
Thibault	Thibault		
WDAGUtility...		Compte d'utilisateur géré par l'administrateur système	

Figure 2 : Création des utilisateurs locaux au Serveur

Iusrmgr - [Utilisateurs et groupes locaux (local)\Groupes]

Fichier Action Affichage ?

Utilisateurs et groupes locaux (local)

- Utilisateurs
- Groupes

Nom	Description	Actions
Administrateurs	Les membres du groupe Administrateurs ont tous les droits sur l'ordinateur.	Groupes
Administrateurs Hyp...	Les membres de ce groupe disposent de tous les droits sur les ressources partagées.	
Duplicateurs	Prend en charge la réPLICATION des utilisateurs.	
IIS_IUSRS	Groupe intégré utilisé par les services Internet.	
Invités	Les membres du groupe Invités n'ont pas accès à l'ordinateur.	
Lecteurs des journaux...	Des membres de ce groupe peuvent lire les journaux.	
Opérateurs d'assistan...	Les membres de ce groupe peuvent aider à l'administration de l'ordinateur.	
Opérateurs de chiffre...	Les membres sont autorisés à effacer les données.	
Opérateurs de config...	Les membres de ce groupe peuvent configurer les paramètres de l'ordinateur.	
Opérateurs de sauveg...	Les membres du groupe Opérateurs de sauvegarde peuvent sauvegarder les données.	
Opérateurs matériels...	Les membres de ce groupe peuvent accéder aux périphériques.	
Propriétaires d'appareils	Les membres de ce groupe peuvent être propriétaires d'appareils.	
System Managed Acc...	Les membres de ce groupe sont gérés par le système.	
Utilisateurs	Les utilisateurs ne peuvent pas effectuer d'opérations administratives.	
Utilisateurs avec pouvoirs	Les utilisateurs avec pouvoir sont autorisés à effectuer toutes les opérations.	
Utilisateurs de gestion...	Les membres de ce groupe ont accès à l'interface de gestion.	
Utilisateurs de l'Analy...	Les membres de ce groupe peuvent analyser les données.	
Utilisateurs du Bureau...	Les membres de ce groupe disposent d'un bureau.	
Utilisateurs du journal...	Les membres de ce groupe peuvent consulter les journaux.	
Utilisateurs du modèle...	Les membres sont autorisés à utiliser le modèle.	
Utilisateurs OpenSSH	Les membres de ce groupe peuvent utiliser OpenSSH.	
Administration		
Commerce		
Comptabilité		
Entrepôt		
Marketing		

Figure 3 : Création des Groupes

## Mise en place des permissions et connexion des postes

Les **permissions d'accès** ont ensuite été configurées : chaque groupe dispose de droits de lecture et d'écriture sur son propre dossier, tandis que les autres dossiers leur sont visibles mais inaccessible. Seul le dossier *Commun* reste accessible à tous les utilisateurs (*voir figure 4*).

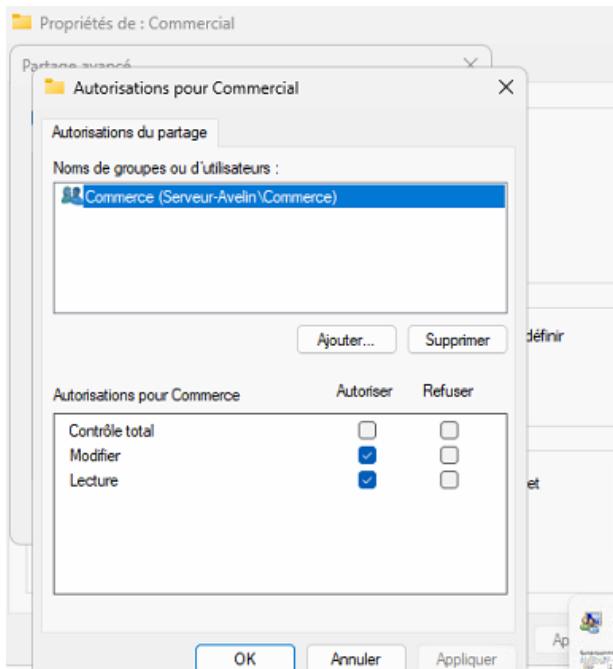


Figure 4 : Paramétrage des permissions.

Une fois la configuration du serveur terminée, j'ai procédé à la **connexion manuelle des 16 postes** de l'entreprise. Sur les ordinateurs Windows, j'ai paramétré l'accès via l'Explorateur de fichiers, tandis que sur les postes macOS, j'ai utilisé la commande *Se connecter au serveur* dans Finder (raccourci ⌘ + K). Chaque utilisateur peut désormais accéder uniquement aux dossiers auxquels il est autorisé.

## Analyse du temps et contraintes rencontrées

Ce projet ne s'est pas limité à une simple mise en place technique. Étant donné que je n'avais **aucune connaissance préalable en administration de serveurs**, j'ai dû consacrer une partie importante du temps à **m'autoformer** et à réaliser des essais sur

machine virtuelle afin d'éviter toute erreur pouvant entraîner une perte de données. Cette étape préparatoire a été essentielle pour comprendre et maîtriser chaque action avant de l'appliquer en production.

Une autre contrainte importante concernait les **horaires d'accès au serveur** : je ne pouvais pas commencer les manipulations avant **11h**, heure à laquelle la personne détenant les accès était présente, alors que mes horaires normaux étaient de **8h à 16h**. Cela a réduit le temps effectif que je pouvais consacrer chaque jour aux tâches techniques.

Malgré ces contraintes et mon manque d'expérience, j'ai réussi à mener à bien ce projet en seulement **7 jours de travail**. Pour comparaison, on peut estimer que ce type de projet représente environ **10 à 15 jours de travail effectif** pour un stagiaire débutant, contre **2 à 3 jours pour un administrateur expérimenté**. "Ce résultat met en avant ma capacité à apprendre rapidement, à m'adapter aux contraintes et à sécuriser mes actions dans un contexte sensible."

## Conclusion et perspectives

Ces différentes étapes m'ont permis de mettre en place un **système centralisé et fonctionnel** : l'ensemble des employés dispose désormais d'un accès adapté à son service, avec des données sécurisées et une meilleure collaboration. Ce projet m'a permis d'acquérir de nouvelles compétences en gestion de serveurs et en administration des permissions, mais aussi de m'adapter à un environnement hétérogène (Windows et macOS) et à travailler dans un contexte avec contraintes techniques et organisationnelles.

Ce travail constitue une **première étape** : à l'avenir, il sera pertinent d'envisager l'ajout d'un second disque dur ou d'un NAS pour séparer le stockage des données du système et d'implémenter une stratégie de sauvegarde automatique. À plus long terme, si l'entreprise acquiert une licence Windows Server, une migration vers un domaine Active Directory pourra également être envisagée.

En conclusion, ce projet représente une **réussite** tant sur le plan technique que sur le plan organisationnel et marque le début d'autres projets informatiques que je poursuivrai dans la continuité de mon stage.

## **Figures proposées :**

- Figure 1 : Schéma de l’arborescence des dossiers.
- Figure 2 : Création des utilisateurs locaux au Serveur
- Figure 3 : Création des Groupes par Service
- Figure 4 : Paramétrage des permissions.
- Figure 5 : Connexion d’un poste utilisateur au partage.

<b>Plateforme</b>	<b>Action</b>	<b>Objectif</b>	<b>Exemple exact utilisé</b>
Windows	Supprimer toutes les connexions précédentes	Déconnecter les partages existants pour reconnecter	net use * /delete
Windows	Connecter un poste au partage réseau	Mapper le dossier partagé sur le poste client	net use Z: \\\u00e2veur-Avelin\Partage /user:Nom Motdepasse
macOS	Se connecter au serveur (Finder → Aller → Se connecter au serveur)	Monter le partage SMB sur Mac	smb://Serveur-Avelin/Partage

# **Chapitre II : Audit de cybersécurité du système informatique**

## **1. Contexte et périmètre**

Dans le cadre de mon stage, et afin de compléter le rapport sur la gestion des dossiers partagés, un audit de cybersécurité a été réalisé pour évaluer l'état global des systèmes informatiques de l'entreprise et identifier les vulnérabilités existantes. L'environnement audité comprend un serveur physique, seize postes clients (14 Windows, 2 macOS), l'infrastructure réseau, ainsi que les services cloud utilisés par les employés (OnePoint et Akead). Le réseau comprend une box Orange, un switch et un routeur, et aucun Wi-Fi invité n'est disponible. Tous les postes Windows sont utilisés avec des comptes standards, limitant les droits administratifs, et l'accès aux services cloud est organisé par rôle, avec un dossier commun accessible à tous.

## **2. Méthodologie**

L'approche suivie reposait sur plusieurs étapes complémentaires. La première étape consistait à inventorier tous les équipements et services, en notant les systèmes d'exploitation, les antivirus présents, les droits utilisateurs et les configurations réseau.

La deuxième étape portait sur l'analyse technique, évaluant l'état des mises à jour des postes et du serveur, la présence et l'efficacité des antivirus, les permissions sur les dossiers partagés, ainsi que la sécurité du réseau et des services cloud. Les points à confirmer incluent l'activation du chiffrement FileVault sur les Mac et la mise en place de l'authentification multi-facteurs sur le cloud.

La troisième étape était l'analyse organisationnelle, portant sur la gestion des comptes utilisateurs, la complexité des mots de passe, la sensibilisation des employés aux risques de phishing et l'existence de procédures de sauvegarde fiables. Enfin, les résultats ont été comparés aux recommandations de l'ANSSI et aux bonnes pratiques ISO 27001 pour proposer un plan d'action priorisé.

## **3. Analyse de l'infrastructure serveur**

Le serveur fonctionne sous Windows 11 avec permissions NTFS correctement configurées, empêchant l'accès général aux fichiers sensibles. Cependant, il n'est pas intégré à un Active Directory, aucune politique de mot de passe n'est définie, et aucun antivirus n'a été identifié. Les mises à jour automatiques et la sauvegarde ne sont pas confirmées. L'accès physique au serveur est libre, la porte restante constamment ouverte, ce qui constitue un risque majeur.

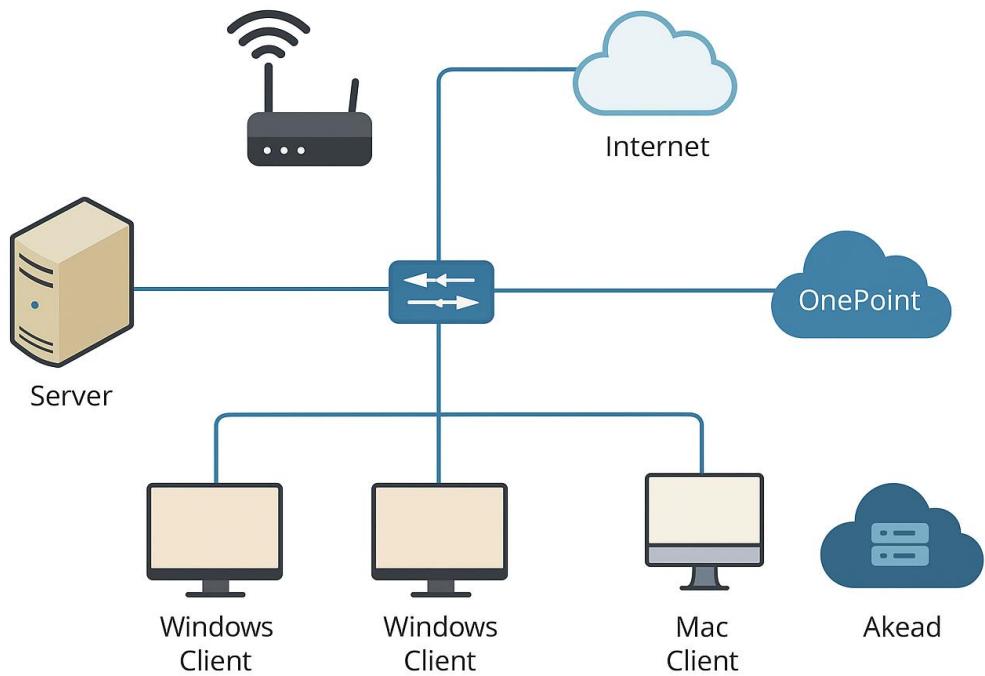


Figure 1 : Schéma de l'infrastructure réseau

## Analyse de la sécurité du système informatique

### 4. Analyse des postes de travail

L'analyse des postes de travail a révélé une configuration relativement homogène sur les machines Windows. Tous les postes sont utilisés avec des comptes standards, ce qui limite les risques liés à l'installation de logiciels malveillants. De plus, Windows Defender est activé par défaut, offrant une protection de base contre les menaces courantes. Toutefois, il reste nécessaire de confirmer que les mises à jour automatiques sont bien activées sur l'ensemble des postes, afin de garantir une protection continue contre les vulnérabilités connues.

Les deux postes macOS présentent quant à eux des failles plus préoccupantes. Aucun antivirus n'est installé, et le chiffrement FileVault n'est pas activé, ce qui expose les données à des risques en cas de vol ou de compromission physique. Bien que les mises à jour soient effectuées régulièrement, l'absence de chiffrement et de protection

antivirus constitue une faiblesse importante dans la sécurité globale du parc informatique.

## 5. Analyse du réseau

L'infrastructure réseau repose sur une box Orange, un switch et un routeur. Aucun réseau Wi-Fi invité n'est disponible, ce qui limite les risques d'intrusion via des connexions non maîtrisées. Cependant, plusieurs éléments doivent être vérifiés pour garantir la sécurité du réseau : la robustesse des mots de passe administrateurs, le filtrage des ports inutiles, et le niveau de chiffrement du Wi-Fi (WPA2 ou WPA3). Par ailleurs, la segmentation du réseau interne n'a pas été confirmée, alors même que les switches Aruba 1830 utilisés sont manageable et permettent la configuration de VLAN et d'ACL. L'absence de segmentation représente un risque d'accès non autorisé entre les différents services.

## 6. Analyse des services cloud

Les services cloud utilisés par l'entreprise sont OnePoint pour la messagerie et Akead pour la gestion documentaire. Les accès sont organisés par rôle, ce qui constitue une bonne pratique en matière de gestion des droits. Toutefois, aucun mécanisme d'authentification multi-facteurs (MFA) n'est activé, ce qui expose les comptes à des risques de compromission en cas de vol de mot de passe. De plus, la sauvegarde externe des données n'a pas pu être confirmée, et l'application Akead, bien qu'installée localement, ne dispose pas de sauvegarde automatique fiable. Ces lacunes compromettent la résilience des données en cas d'incident.

## 7. Organisation et gestion des accès

La gestion des comptes utilisateurs est entièrement manuelle, sans procédure formalisée. Aucune politique de mots de passe n'est définie, et les utilisateurs ne sont pas sensibilisés aux risques liés au phishing. Ces lacunes augmentent considérablement les risques d'attaques par ingénierie sociale et de compromission des identifiants. L'absence de formation ou de test de vigilance constitue un point critique dans la posture de sécurité de l'entreprise.

## 8. Analyse des risques et recommandations

Le serveur principal fonctionne sous Windows 11 et bénéficie de permissions NTFS correctement configurées, ce qui limite les accès non autorisés aux fichiers sensibles. Toutefois, l'accès physique au serveur n'est pas sécurisé : la porte de la salle reste ouverte en permanence, exposant l'infrastructure à des risques d'intrusion, de vol ou

de sabotage. La criticité de cette vulnérabilité est très élevée. Il est donc impératif de sécuriser l'accès physique, d'installer un antivirus, d'activer les mises à jour automatiques, et de mettre en place une stratégie de sauvegarde régulière et externalisée.

Les postes Windows, bien configurés en termes de droits utilisateurs, nécessitent une vérification des mises à jour automatiques et du bon fonctionnement de l'antivirus. Les postes macOS doivent impérativement être équipés d'un antivirus et bénéficier du chiffrement FileVault, en plus d'une vérification des mises à jour.

Le réseau doit être renforcé par la modification des mots de passe administrateurs, le filtrage des ports inutiles, et l'activation du chiffrement WPA2 ou WPA3. La mise en place d'un Wi-Fi invité isoler et la configuration de VLAN sur les switches Aruba permettraient de segmenter les flux et de limiter les risques d'accès non autorisé.

Les services cloud doivent intégrer une authentification multi-facteurs pour tous les comptes, et une sauvegarde externe régulière doit être mise en place pour garantir la résilience des données. Une politique de mots de passe forte, avec rotation régulière, doit être imposée à tous les utilisateurs, et une procédure claire de création, modification et suppression des comptes doit être formalisée.

Enfin, la sensibilisation des employés aux risques de phishing doit devenir une priorité. Des formations courtes, des supports pédagogiques et des tests de simulation réguliers permettront de renforcer la vigilance collective et de réduire les risques liés à l'ingénierie sociale.

## **9. Comparaison avec les normes de sécurité**

La comparaison avec les normes internationales confirme les lacunes identifiées. Selon la norme ISO/IEC 27001, plusieurs non-conformités sont observées, notamment l'absence de politique de mots de passe, de MFA, de sauvegarde externalisée, et de contrôle physique du serveur. Le cadre NIST Cybersecurity Framework révèle des lacunes sur les fonctions Identify, Protect et Recover, tandis que les CIS Controls v8 montrent une conformité partielle sur les droits administrateurs, mais des insuffisances sur la gestion des accès et la sauvegarde des données.

En résumé, l'entreprise présente une adoption partielle des bonnes pratiques de sécurité, avec des faiblesses critiques sur la sauvegarde, l'authentification forte, le chiffrement des postes macOS et la sécurité physique du serveur.

## **10. Conclusion et recommandations**

L'audit met en évidence une infrastructure simple mais fragile. Les points forts incluent la gestion correcte des permissions et l'utilisation de comptes standards sur les postes Windows. En revanche, les faiblesses critiques concernent la sécurité physique du serveur, la protection des postes Mac, la complexité des mots de passe, l'absence de MFA et de sensibilisation au phishing.

Il est donc recommandé de mettre en place des sauvegardes automatiques et externalisées pour le serveur et l'application Akead, d'activer l'authentification multi-facteurs sur les services cloud, de sécuriser physiquement le serveur, d'activer FileVault et un antivirus sur les postes macOS, de créer un réseau Wi-Fi invité isoler, de formaliser une politique de mots de passe et une procédure de gestion des comptes, et enfin de former les employés aux bonnes pratiques de cybersécurité. La mise en œuvre de ces mesures permettra de réduire significativement les risques de compromission et de perte de données, tout en instaurant une culture de sécurité pérenne au sein de l'entreprise.

## **Mise en œuvre des solutions de sécurité**

### **11 Objectif du rapport de solutions**

À la suite de l'audit de cybersécurité réalisé chez InterResto, un rapport de solutions a été rédigé afin de proposer une architecture de sécurité progressive, adaptée aux besoins réels de l'entreprise et à ses contraintes budgétaires. Ce rapport vise à corriger les failles identifiées dans l'audit, à renforcer la résilience des données critiques, et à poser les bases d'une infrastructure informatique plus robuste, évolutive et conforme au RGPD.

### **12 Correspondance entre failles et solutions proposées**

Chaque solution technique a été pensée pour répondre à une faille précise identifiée lors de l'audit :

<b>Failles identifiées</b>	<b>Solutions proposées</b>
Absence de sauvegarde centralisée	NAS Synology DS923+ avec disques en RAID 1 + sauvegarde cloud OVH
Pas d'antivirus professionnel	Bitdefender GravityZone (20 postes) avec console centralisée

Pas de pare-feu dédié	Stormshield SN170 avec licence UTM 3 ans
Pas d'Active Directory	Windows Server Essentials + configuration AD
Risques sur les postes macOS	Installation d'un antivirus + activation de FileVault
Absence de MFA sur les services cloud	Activation de l'authentification multi-facteurs sur OnePoint et Akead
Accès physique non sécurisé au serveur	Verrouillage de la salle serveur
Absence de segmentation réseau	Configuration de VLAN sur les switches Aruba 1830
Aucune sensibilisation des utilisateurs	Mise en place de formations et de tests de phishing

## 13 Architecture cible par phase

Le déploiement des solutions a été organisé en deux phases pour respecter les priorités de sécurité et la capacité d'investissement de l'entreprise :

### ***Phase 1 : sécurisation des données et des postes***

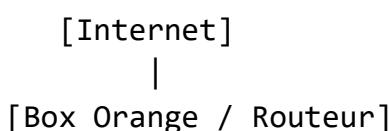
- Mise en place d'un NAS Synology DS923+ avec 2 disques de 4 To en RAID 1
- Sauvegarde automatique vers le cloud OVH
- Installation de Bitdefender GravityZone sur 20 postes
- Structuration du réseau local (préparation des VLAN)
- Maintien temporaire du poste Windows 11 comme serveur de fichiers

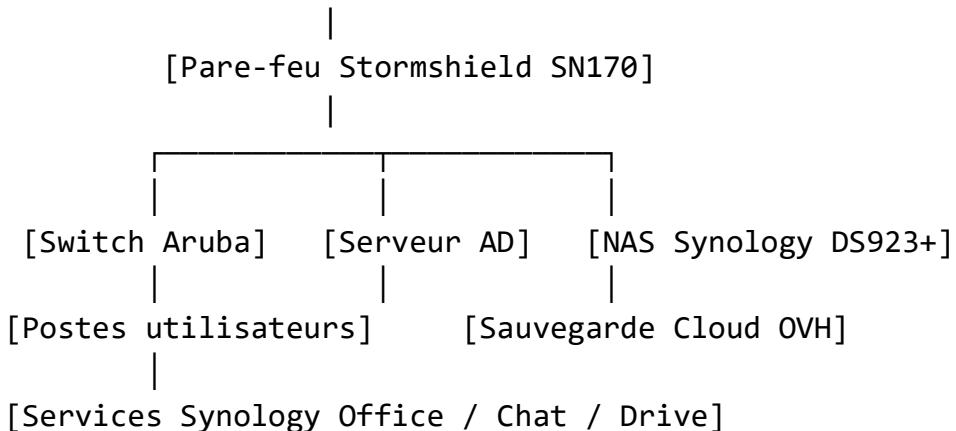
### ***Phase 2 : sécurisation du périmètre et gestion centralisée***

- Installation d'un pare-feu Stormshield SN170 avec licence UTM 3 ans
- Déploiement d'un serveur Windows Server Essentials avec Active Directory
- Centralisation des comptes utilisateurs et des droits d'accès
- Activation de l'authentification forte (MFA) sur les services cloud
- Sécurisation physique de la salle serveur

## 14 Schéma d'architecture cible

Ce schéma illustre l'architecture cible proposée :





Cette architecture permet :

- Une segmentation réseau via VLAN
- Une centralisation des données et des accès
- Une protection périphérique renforcée
- Une sauvegarde locale et externe
- L'intégration de services collaboratifs internes

## 15 Justification du choix des solutions

Les solutions retenues ont été sélectionnées pour leur fiabilité, leur compatibilité avec l'environnement existant, et leur adéquation avec les besoins d'une PME de 16 postes. Le NAS DS923+ offre une excellente évolutivité, avec la possibilité d'ajouter des baies, de la RAM, et des SSD NVMe pour accélérer les accès. Le pare-feu Stormshield SN170 est un modèle fanless, silencieux et certifié, parfaitement adapté à une structure de moins de 25 utilisateurs. L'Active Directory permettra de centraliser les accès, de renforcer la traçabilité, et de préparer l'entreprise à de futures exigences réglementaires.

## 16 Compétences mobilisées

Ce projet m'a permis de mobiliser un large éventail de compétences techniques et organisationnelles :

<b>Compétence</b>	<b>Mise en œuvre concrète</b>
Audit de sécurité	Analyse des postes, réseau, cloud, accès
Gestion de projet technique	Phasage des solutions, priorisation, budgétisation
Configuration système	NAS Synology, dossiers partagés, droits d'accès
Documentation technique	Rédaction du rapport de solutions, procédures
Communication stratégique	Présentation au PDG, vulgarisation des enjeux
Conformité RGPD	Journalisation, segmentation, sauvegarde externalisée
Sécurité réseau	Préparation VLAN, choix du pare-feu Stormshield
Sensibilisation utilisateur	Recommandations sur MFA, phishing, mots de passe
Esprit d'analyse	Justification des choix techniques et budgétaires
Autonomie et initiative	Proposition de solutions adaptées au contexte PME

## 17 Mon rôle dans la mise en œuvre

En tant que stagiaire, j'ai activement participé à la mise en œuvre des solutions proposées. Mes contributions ont inclus :

- L'analyse des besoins techniques et la rédaction du rapport de solutions
- La sélection du modèle de NAS et la justification technique du DS923+
- La configuration initiale du NAS, des dossiers partagés et des droits d'accès
- La planification de la migration des données depuis le poste Windows 11
- La documentation des procédures de sauvegarde et de restauration
- La préparation de la configuration réseau (VLAN, segmentation)
- La présentation des solutions au PDG

## 18 Résultats attendus

La mise en œuvre progressive de ces solutions permettra à InterResto de :

- Sécuriser ses données critiques contre les pertes, les attaques et les erreurs humaines
- Améliorer la conformité RGPD grâce à une meilleure traçabilité et à une gestion centralisée des accès
- Renforcer la résilience de son infrastructure en cas d'incident
- Offrir un environnement de travail plus fiable et plus professionnel aux employés

- Poser les bases d'une évolution future vers des services collaboratifs internes (Synology Office, Chat, Calendar)

## 19 Conclusion

Ce projet m'a permis de mobiliser l'ensemble des compétences acquises durant ma formation d'ingénieur, en les confrontant à une problématique réelle d'entreprise. De l'audit à la mise en œuvre, j'ai pu proposer des solutions concrètes, sécurisées et évolutives, tout en tenant compte des contraintes budgétaires et humaines. Cette expérience m'a également permis de développer mes capacités de communication, de structuration technique, et de prise de décision. Elle constitue une étape clé dans mon parcours vers une ingénierie responsable, tournée vers la sécurité, l'efficacité et l'impact.

# Annexe A : Audit de cybersécurité

## 1. Contexte et périmètre

L'audit de cybersécurité a été réalisé afin d'évaluer l'état actuel des pratiques de sécurité informatique au sein de l'entreprise et d'identifier les risques majeurs. L'infrastructure observée se compose d'un serveur physique sous Windows 11, de seize postes de travail (principalement Windows, avec deux postes macOS), d'un réseau interne connecté à une box Orange, comprenant un Wi-Fi Interresto protégé par mot de passe et des switches Aruba 1830 manageable, ainsi que des solutions de messagerie (OnePoint) et une application locale métier (Akead). L'audit a également porté sur les aspects organisationnels, tels que la gestion des comptes et des droits, la politique de sauvegarde et la sensibilisation des utilisateurs.

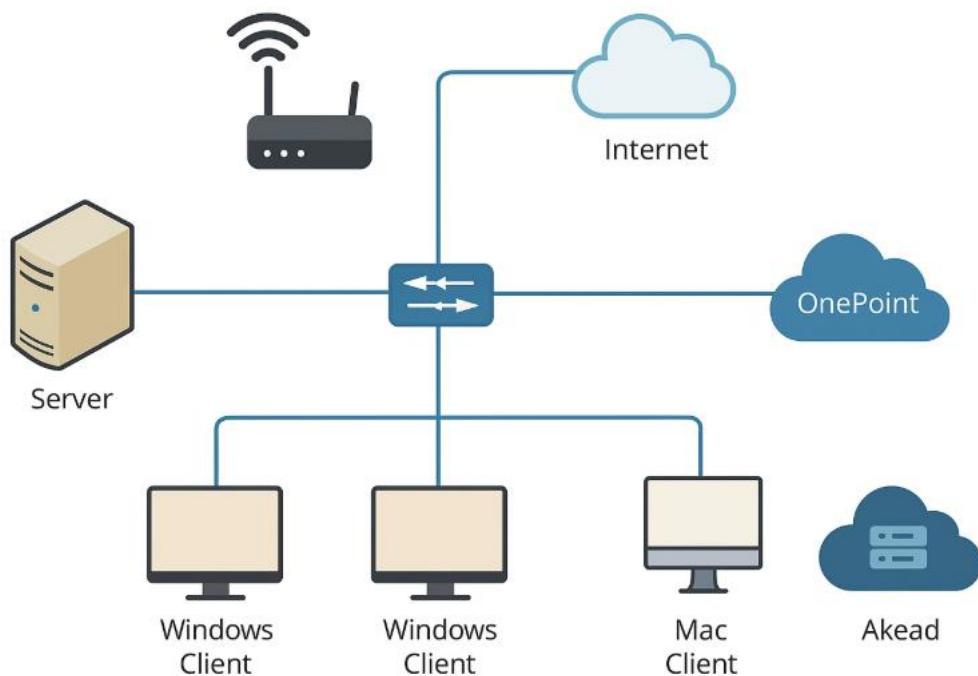


Figure 1 : Schéma de l'environnement

## 2. Analyse de l'infrastructure serveur

Le serveur fonctionne sous Windows 11 et assure des fonctions centrales pour le stockage et l'accès aux données. Bien que BitLocker soit activé et que les sauvegardes automatiques soient en place, la politique de mots de passe n'est pas définie, ce qui représente un risque important en termes de sécurité des identités. Le serveur est également situé dans une pièce accessible, sans contrôle physique strict, ce qui constitue une vulnérabilité en cas de tentative d'accès non autorisé. Les mises à jour Windows sont appliquées régulièrement, garantissant une protection contre les vulnérabilités connues.

Recommandations :

- Définir une politique de mots de passe robuste (longueur minimale, complexité, expiration).
- Restreindre l'accès physique au serveur.
- Vérifier la sécurité et la fréquence des sauvegardes automatiques.



Figure 2 : Accès simple à la salle du Serveur

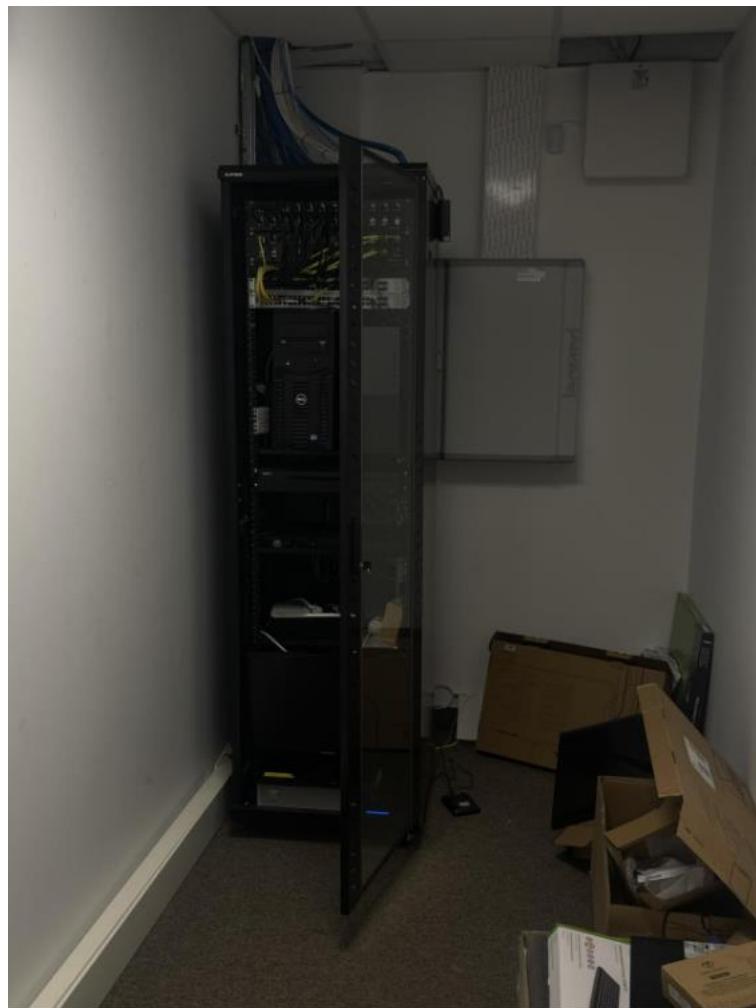


Figure 3 : Accès au terminal du Serveur

### 3. Analyse des postes de travail

#### 3.1 Postes Windows

Les postes Windows présentent une sécurité de base correcte : Windows Defender est activé et à jour, les mises à jour automatiques sont fonctionnelles, et les utilisateurs disposent de comptes standards, limitant le risque d'installation de logiciels malveillants. Un comportement observé dans l'entreprise est que la majorité des utilisateurs de postes Windows laissent leur session ouverte lorsqu'ils quittent leur poste de travail, parfois même en fin de journée.

Ce type de pratique représente un risque important en matière de sécurité, car toute personne ayant un accès physique au poste peut utiliser la session sans authentification. Cela expose l'entreprise à des risques de fuite de données, d'usurpation d'identité ou de malveillance interne.

### 3.2 Postes macOS

Les deux postes macOS présentent une vulnérabilité notable : FileVault n'est pas activé, ce qui expose les données en cas de vol ou perte de l'ordinateur. Les mises à jour sont effectuées régulièrement et les comptes sont également standards. Concernant les utilisateurs de postes MacOs, le respect des bonnes pratiques est globalement plus élevé que sur les postes Windows, notamment en ce qui concerne la fermeture ou le verrouillage de la session. Ce comportement limite significativement les risques liés à l'accès non autorisé en cas d'absence de l'utilisateur.

Recommandations :

- Activer FileVault sur tous les postes macOS.
- Vérifier qu'aucun compte temporaire ou partagé n'existe.
- Maintenir la régularité des mises à jour.
- Mettre en place une stratégie technique telle que la **fermeture automatique de session après un temps d'inactivité** (GPO ou configuration locale)

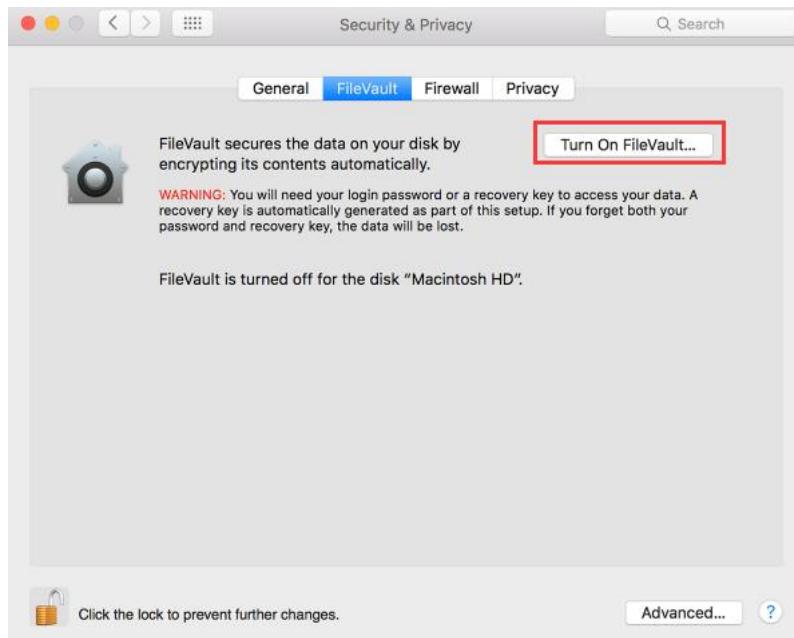


Figure 4 : Non activation de FileVault

### 4. Analyse du réseau

Le réseau interne repose sur une box Orange, un Wi-Fi Interresto protégé par mot de passe et des switches Aruba 1830 manageable. Ces switches permettent la

configuration de VLAN et d'ACL, offrant la possibilité de segmenter le réseau et d'isoler les flux critiques.

- À ce stade, il n'a pas été vérifié si des VLAN ou ACL sont effectivement configurés, ce qui constitue un point à confirmer.
- Le firmware des switches et de la box doit être maintenu à jour pour garantir la sécurité.

Recommandations :

- Vérifier et configurer la segmentation réseau sur les switches Aruba.
- Maintenir les mises à jour du firmware.

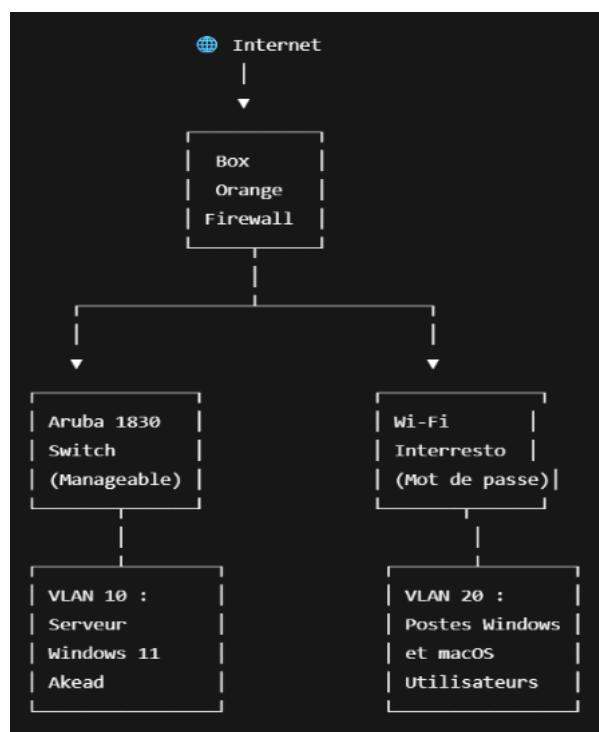


Figure 5 : Schéma de l'architecture réseau interne avec segmentation VLAN et Wi-Fi Inter Resto

Explication :

- La Box Orange assure la connexion internet et le pare-feu principal.
- Le switch Aruba 1830 est manageable et permet de configurer des VLAN pour isoler le serveur (VLAN 10) des postes de travail (VLAN 20).
- Le Wi-Fi Inter Resto est protégé par mot de passe, mais il serait recommandé de le placer dans un VLAN séparé pour isoler les invités du réseau interne.
- Chaque VLAN peut être contrôlé via le switch pour limiter les flux et appliquer des règles de sécurité.

## 5. Analyse des solutions cloud

La solution OnePoint est utilisée pour la **messagerie et Akead pour la gestion documentaire et organisationnelle**. Cependant :

- MFA n'est pas activé → vulnérabilité critique.
- La robustesse des mots de passe et la présence de journaux d'audit restent à vérifier.

Recommandations :

- Activer MFA pour tous les comptes.
- Vérifier la politique de mots de passe et la tenue des journaux d'audit.

## 6. Analyse de l'application locale Akead

Akead dispose d'une sauvegarde automatique, ce qui est positif pour la continuité d'activité. Cependant :

- La fréquence et le stockage externe des sauvegardes doivent être confirmés.
- Aucun mécanisme de MFA n'est disponible, exposant l'application à un risque critique de compromission en cas de vol de mot de passe.
- Il est recommandé de tester régulièrement les procédures de restauration des données.

Recommandations :

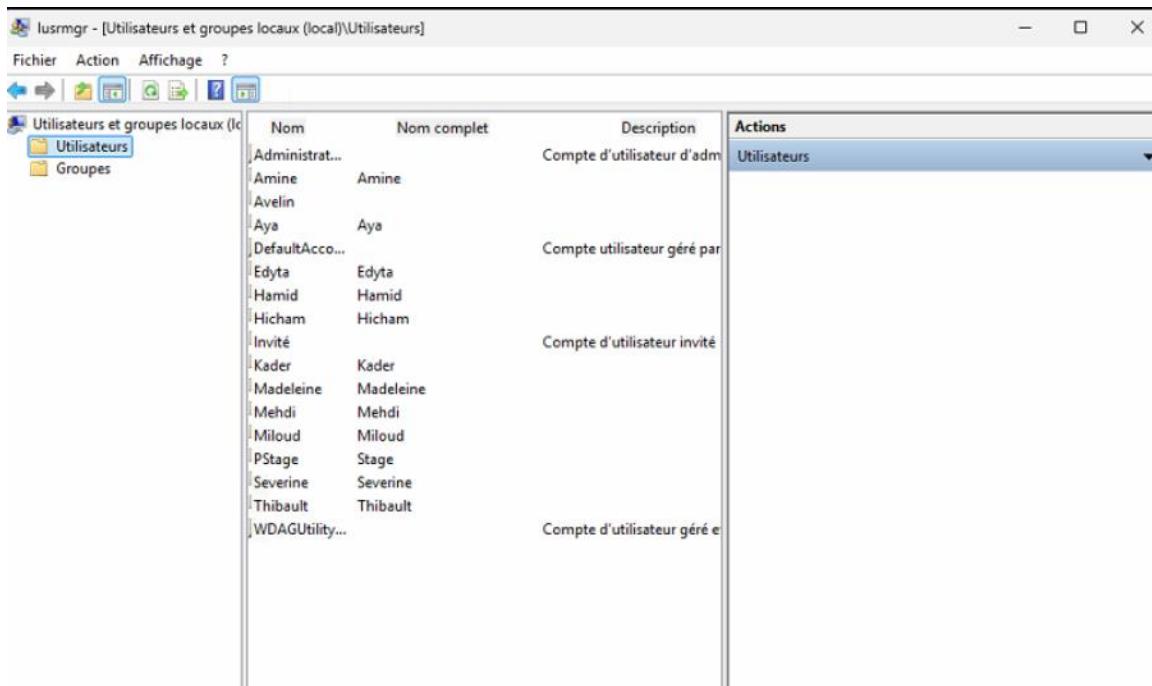
- Confirmer fréquence et stockage des sauvegardes.
- Activer MFA ou solution équivalente.
- Effectuer des tests de restauration périodiques.

## 7. Gestion des accès et comptes utilisateurs

L'entreprise ne dispose pas d'une politique centralisée de mots de passe, et aucun Active Directory n'est déployé. Cela limite la capacité à appliquer des règles uniformes et à contrôler les accès. Certains comptes inactifs subsistent sur le serveur. Les permissions NTFS et la gestion par rôles offrent une protection partielle mais non centralisée.

Recommandations :

- Mettre en place Active Directory ou une politique manuelle stricte.
- Supprimer ou désactiver les comptes inactifs.
- Suivi régulier des permissions et droits d'accès.



The screenshot shows the Windows Local Users and Groups Management console window titled "lusrmgr - [Utilisateurs et groupes locaux (local)\Utilisateurs]". The left pane displays a tree view with "Utilisateurs et groupes locaux (local)" expanded, showing "Utilisateurs" and "Groupes". The right pane is a grid table with columns: "Nom", "Nom complet", "Description", and "Actions". The "Actions" column dropdown is set to "Utilisateurs". The table lists the following user accounts:

Nom	Nom complet	Description	Actions
Administrat...		Compte d'utilisateur d'admin	Utilisateurs
Amine	Amine		
Avelin			
Aya	Aya		
DefaultAcco...		Compte utilisateur géré par l'administrateur	
Edyta	Edyta		
Hamid	Hamid		
Hicham	Hicham		
Invité		Compte d'utilisateur invité	
Kader	Kader		
Madeleine	Madeleine		
Mehdi	Mehdi		
Miloud	Miloud		
PStage	Stage		
Severine	Severine		
Thibault	Thibault		
WDAGUtility...		Compte d'utilisateur géré par l'administrateur	

Figure 7 : Gestion des accès et comptes utilisateurs

## 8. Sensibilisation et gestion des menaces

Aucune formation ou sensibilisation structurée n'a été mise en place pour les utilisateurs. Le filtrage anti-phishing est inexistant, et les enregistrements SPF/DKIM/DMARC ne sont pas configurés, ce qui expose l'entreprise à des attaques par phishing ou spoofing. Les employés ont déjà signalé des courriels suspects, confirmant la vulnérabilité.

Recommandations :

- Former les utilisateurs aux bonnes pratiques de sécurité.
- Mettre en place un filtrage anti-phishing.
- Configurer SPF, DKIM et DMARC pour sécuriser les Emails.

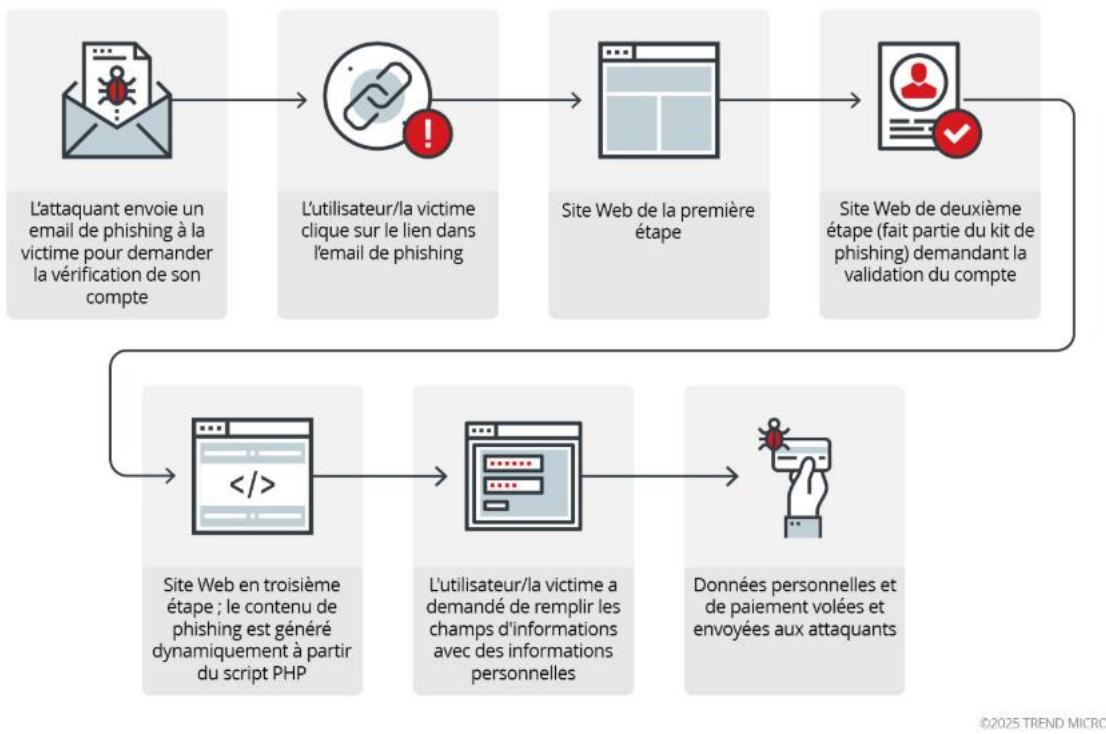


Figure 8 : Chaîne d'infection de l'attaque de phishing de Heatstroke ; notez que la chaîne d'infection peut changer en fonction des propriétés de l'utilisateur/du comportement

## 9. Tableau synthétique des risques et priorisation

	Élément / Risque	Criticité	Priorité	Commentaire
1	MFA non activé sur OnePoint	⚠ Critique	Haute	Vulnérabilité majeure en cas de phishing Accès aux données sensibles possible avec mot de passe compromis
2	MFA non activé sur Akead	⚠ Critique	Haute	Risque de fuite de données en cas de vol/perte
3	FileVault non activé sur macOS	⚠ Elevée	Moyenne	Comptes faibles ou expirés exposés
4	Politique de mots de passe inexistante	⚠ Critique	Haute	Risque d'accès direct aux données et
5	Accès physique au serveur non restreint	⚠ Elevée	Moyenne	

6	Filtrage anti-phishing non actif	⚠️ Élevée	Moyenne	modification de configurations Exposition aux emails frauduleux
7	SPF/DKIM/DMARC non configurés	⚠️ Élevée	Moyenne	Risque de spoofing / phishing sur le domaine
8	Sauvegardes Akead – fréquence à confirmer	⚠️ Élevée	Moyenne	Risque de perte de données si corruption ou incident
9	Segmentation VLAN non vérifiée sur Aruba 1830	⚠️ Moyenne	Basse	Limite la sécurité réseau et isolation des flux
10	Comptes inactifs sur serveur	⚠️ Moyenne	Moyenne	Accès non autorisé possible

## 10. Checklist technique rapide

Élément	Vérification	État	Commentaires
Serveur Windows 11	Sauvegarde automatique	Oui	Vérifier fréquence et stockage
Serveur Windows 11	BitLocker	Oui	-
Serveur Windows 11	Politique mots de passe	Non	Définir règles robustes
Poste Windows	Defender activé	Oui	-
Poste Windows	Mises à jour automatiques	Oui	-
Poste macOS	FileVault	Non	Activer pour sécuriser données
Poste macOS	Mises à jour	Oui	-
Poste macOS	Compte standard	Oui	-
Wi-Fi Interresto	Mot de passe activé	Oui	Vérifier isolation réseau si possible
Aruba 1830	Manageable	Oui	VLAN / ACL à vérifier

OnePoint	MFA	Non	Activer immédiatement
Akead	Sauvegarde automatique	Oui	Confirmer fréquence et stockage
Akead	MFA	Non	Activer ou méthode équivalente
Emails	Anti-phishing	Non	Mettre en place
Emails	SPF/DKIM/DMARC	Non	Configurer
Utilisateurs	Sensibilisation	Non	Prévoir formation

## 11. Alignement avec les normes de sécurité

L'audit met en évidence un certain nombre d'écart par rapport aux bonnes pratiques définies dans les référentiels internationaux.

### 1. ISO/IEC 27001

Cette norme internationale définit un système de management de la sécurité de l'information (SMSI) et fixe des bonnes pratiques pour protéger les données et les systèmes.

Les points relevés :

- **Gestion des accès (absence de politique de mots de passe et de MFA)**
  - L'entreprise n'a pas de règles claires sur la complexité, la durée de vie ou le renouvellement des mots de passe, et elle n'utilise pas d'authentification multi-facteurs.
  - Cela augmente fortement le risque que des comptes soient piratés, car un mot de passe simple ou compromis peut donner un accès total aux ressources critiques.
- **Sauvegarde (absence de stratégie systématique et externalisée)**
  - Les données du serveur ne sont pas sauvegardées régulièrement ni stockées hors site.

- En cas de panne, d'attaque ou de perte de matériel, il est possible que les données soient irrécupérables.
- **Sécurité physique (serveur accessible sans contrôle)**
  - Le serveur est dans une pièce dont la porte est ouverte en permanence.
  - N'importe qui peut y accéder physiquement, ce qui permettrait à une personne malveillante de copier, modifier ou supprimer des données.

## 2. NIST Cybersecurity Framework (CSF)

Il s'agit d'un référentiel américain organisant la cybersécurité en 5 fonctions Identify (identifier), Protect (protéger), Detect (détecter), Respond (réagir) et Recover (récupérer).

- Les lacunes relevées :
  - **Identify (cartographie des actifs incomplète)**
    - L'entreprise ne connaît pas tous ses systèmes, logiciels et données critiques.
    - Sans cette connaissance, il est difficile de sécuriser les ressources importantes et de prioriser la protection.
  - **Protect (absence de chiffrement sur macOS et MFA)**
    - Les postes macOS ne sont pas chiffrés avec FileVault et aucune authentification multi-facteurs n'est mise en place sur les applications critiques.
    - Cela facilite l'accès aux données pour un attaquant qui obtiendrait un mot de passe ou un appareil volé.
  - **Respond/Recover (absence de plan d'incident et de reprise)**
    - L'entreprise n'a pas de procédure formelle pour réagir en cas de cyberattaque ni de plan pour restaurer les données après un incident.

→ Chaque incident pourrait être désorganisé, long à résoudre, voire entraîner une perte de données ou d'activité.

### 3. CIS Controls v8

Ce référentiel regroupe 18 mesures essentielles de sécurité informatique.

- **Contrôle 4 – Gestion des droits administrateurs : OK**

→ Les utilisateurs n'ont pas de droits administrateurs sur leurs postes, ce qui réduit le risque d'installation de logiciels malveillants ou de modification des paramètres critiques.

- **Contrôle 6 – Gestion des accès : Partiellement conforme**

→ L'absence de politique de mots de passe et de MFA reste un problème, exposant l'entreprise à des risques d'accès non autorisés.

- **Contrôle 11 – Sauvegarde des données : Partiellement conforme**

→ Les sauvegardes automatiques et externalisées ne sont pas mises en place pour le serveur, ce qui constitue un risque majeur en cas d'incident.

Résumé, l'organisation se situe aujourd'hui à un niveau de maturité faible au regard des normes internationales, avec certaines bonnes pratiques présentes, mais des lacunes critiques sur la sauvegarde, l'authentification forte et la sécurité physique. On considère cela normal aux vues de la taille de l'entreprise et des données traiter, mais des améliorations sont à envisager.

## 12. Conclusion et recommandations

L'audit révèle une infrastructure simple mais présentant plusieurs points de fragilité critique, notamment :

- Absence de MFA sur OnePoint et Akead.
- Absence de chiffrement FileVault sur macOS.
- Politique de mots de passe inexistante et comptes inactifs.
- Filtrage anti-phishing

# Annexe B : Solutions Audit Cyber – InterResto

## 1. Introduction

InterResto est un grossiste alimentaire dont les données critiques incluent :

- Informations comptables
- Données clients
- Tarifs et marges des marchandises

Ces données sont sensibles et doivent être protégées contre les risques informatiques (ransomware, vol, erreur humaine) et conformes au RGPD. L'objectif de cet audit est de proposer une **stratégie de sécurisation progressive**, adaptée aux besoins réels et au budget de l'entreprise.

## 2. Analyse de l'existant et justification des non-choix

### ◊ Absence de pare-feu

#### Situation actuelle

Le réseau est uniquement protégé par une box Orange. Aucun pare-feu professionnel n'est en place. Les accès distants se font via TeamViewer, souvent laissé ouvert.

#### Pourquoi ce n'est pas acceptable

- La box ne filtre pas les flux ni les tentatives d'intrusion
- TeamViewer n'est pas conçu pour un usage sécurisé en entreprise
- Aucun journal d'accès, aucune segmentation du réseau

#### Conclusion

Cette configuration expose l'entreprise à des risques majeurs (ransomware, vol de données) et n'est pas conforme aux exigences RGPD.

## ◊ Pare-feu logiciel (pfSense, OPNsense)

### Constat

Des solutions open source existent, installables sur un mini-PC.

### Pourquoi ce n'est pas retenu

- Pas de garantie matérielle (PC non durci, non certifié)
- Maintenance complexe, sans support professionnel
- Pas de sécurité unifiée (pas d'antivirus réseau, pas d'IPS/IDS intégrés)
- Non-conformité RGPD (pas de journalisation certifiée)

### Conclusion

Ce type de solution peut convenir à un usage personnel ou technique, mais pas à une PME sans service informatique.

## ◊ Aucune sauvegarde

### Constat

Les données critiques (comptabilité, RH, clients) sont réparties sur les postes. Aucun NAS, aucun cloud, aucun plan de restauration.

### Pourquoi ce n'est pas retenu

- Risque total en cas de panne, attaque ou erreur humaine
- Non-conformité RGPD : absence de protection des données personnelles

### Conclusion

L'absence de sauvegarde est un risque majeur. Une solution NAS + cloud est indispensable.

## ◊ Aucun antivirus

### Constat

Les postes ne sont pas protégés contre les malwares ou ransomwares.

### Pourquoi ce n'est pas retenu

- Risque d'infection par email, clé USB ou site web
- Aucun contrôle centralisé, aucune mise à jour automatique

## Conclusion

Un antivirus professionnel est indispensable.

### ◊ Pas d'Active Directory

## Constat

Les utilisateurs ont des comptes locaux, sans politique de mot de passe ni gestion des droits.

## Pourquoi ce n'est pas retenu

- Impossible de centraliser les accès ou de gérer les permissions
- Non-conformité RGPD : pas de contrôle d'accès structuré

## Conclusion

Un Active Directory est nécessaire.

## 3. Architecture cible par phase

<b>Phase</b>	<b>Objectif</b>	<b>Composants clés</b>
<b>Phase 1</b>	Sécuriser les données et les postes Renforcer la sécurité	NAS Synology + sauvegarde cloud OVH, Bitdefender GravityZone, structuration réseau (VLAN), poste serveur Windows 11
<b>Phase 2</b>	périmétrique et les accès	Pare-feu Stormshield SN170 + licence UTM 3 ans, Windows Server Essentials + Active Directory

## 4. Choix du pare-feu – Stormshield SN170

### ◊ Fiche technique officielle – Stormshield SN170

Caractéristique	Valeur SN170
Débit Firewall	3 Gbps
Débit VPN IPSec	600 Mbps
Interfaces réseau	4 × 2,5 Gbit/s
Connexions simultanées	150 000
Format	Fanless, industriel
Taille entreprise cible	≤ 25 postes

### ◊ Comparaison technique

Critère	SN170	SN220	SN320
Débit Firewall	3 Gbps	4 Gbps	8 Gbps
Débit VPN IPSec	600 Mbps	1 Gbps	2 Gbps
Ports réseau	4 × 2.5 GbE	8 × 2.5 GbE	8 × 2.5 GbE
Connexions simultanées	150 000	300 000	500 000
Format	Fanless	Fanless	Ventilé
Taille entreprise	≤ 25 postes	25–50 postes	50+ postes
VPN / télétravail	Modéré	Avancé	Intensif
Conformité RGPD	Basique	Conforme PME	Conforme audit ISO

### ◊ Comparaison budgétaire

Élément	SN170	SN220	SN320
Appliance seule (HT)	500,00 €	1 254,00 €	1 666,00 €
Licence UTM Premium 3 ans (HT)	996,00 €	996,00 €	996,00 €

Configuration réseau (HT)	660,00 €	660,00 €	660,00 €
<b>Total TTC</b>	<b>2 587,20 €</b>	3 492,00 €	3 986,40 €

#### ◊ Licence 1 an vs 3 ans

Critère	Licence 1 an	Licence 3 ans
Prix annuel moyen	~500 € TTC	~398 € TTC/an
Coût sur 3 ans	~1 500 € TTC	~1 195 € TTC
Économie réalisée	Aucune	~300 €
Renouvellement	Annuel	Tous les 3 ans
Stabilité budgétaire	Faible	Forte

#### Choix recommandé : Stormshield SN170 avec licence 3 ans

Suffisant pour 16 postes, VPN performant, licence complète incluse, boîtier durci, silencieux, budget maîtrisé.

## 5. Sauvegarde automatique – NAS + Cloud

Élément	Prix TTC
NAS Synology DS923+	744,00 €
2 × Disques 4 To (RAID 1)	324,00 €
Sauvegarde cloud OVH	144,00 €
Configuration + test	576,00 €
<b>Total TTC</b>	<b>1 788,00 €</b>

## 6. Antivirus – Bitdefender GravityZone

Élément	Prix TTC
Licence 20 postes	432,00 €

## 7. Active Directory – Windows Server Essentials

Élément	Prix TTC
Licence Windows Server	480,00 €

Configuration AD complète	720,00 €
<b>Total TTC</b>	<b>1 200,00 €</b>

## 8. Synthèse budgétaire par phase

Phase	Domaine	Solution proposée	Budget TTC
<b>Phase 1</b>	Sauvegarde	NAS Synology + disques + cloud + config	1 788,00 €
	Antivirus	Bitdefender GravityZone (20 postes)	432,00 €
<b>Phase 2</b>	Sécurité réseau	Stormshield SN170 + configuration VLAN	2 587,20 €
	Serveur AD	Windows Server Essentials + configuration	1 200,00 €
<b>Total global</b>			<b>6 007,20 €</b>

## 9. Réévaluation de la priorité du pare-feu Stormshield

### ◊ Contexte métier

Les données critiques d'InterResto sont sensibles, mais ne relèvent pas de la catégorie "données hautement confidentielles" (ex. médicales, bancaires). À ce jour, aucun service exposé à Internet (serveur web, accès distant, API publique) n'a été identifié.

### ◊ Analyse technique

- La surface d'attaque externe est limitée
- Les postes de travail sont le vecteur principal d'attaque
- Les données critiques sont mieux protégées par un NAS sécurisé avec sauvegarde cloud
- Le budget peut être optimisé en différant l'achat du pare-feu sans compromettre la sécurité immédiate

## ◊ Recommandation

Il est recommandé de repositionner le Stormshield en **phase 2**, sauf en cas d'évolution du périmètre (accès distant, interconnexion avec partenaires, audit RGPD). En **phase 1**, la sécurité peut être assurée par :

- ◊ NAS Synology avec RAID + sauvegarde OVH
- ◊ Antivirus centralisé

## Annexe C : Charte de sécurité



### 1. ⏹ Objectif

Cette charte vise à sensibiliser les collaborateurs d'Inter Resto aux bonnes pratiques de sécurité informatique afin de protéger les données de l'entreprise, les systèmes d'information et les informations personnelles.

## 2. Mots de passe

### Règles à respecter :

- Utiliser un mot de passe **complexe** : au moins 12 caractères, avec majuscules, minuscules, chiffres et symboles.
- Ne jamais utiliser le même mot de passe sur plusieurs services.
- Changer son mot de passe tous les **6 mois** ou en cas de suspicion de compromission.
- Ne jamais partager son mot de passe, même avec un collègue.
- Ne pas enregistrer les mots de passe dans un fichier non sécurisé ou sur papier.
- Utiliser un **gestionnaire de mots de passe** si nécessaire (ex : Bitwarden, KeePass).

## 3. Phishing et sécurité des emails

### Comportements à adopter :

- Ne jamais cliquer sur un lien ou ouvrir une pièce jointe provenant d'un expéditeur inconnu ou suspect.
- Vérifier l'adresse email de l'expéditeur (attention aux fautes ou aux adresses proches).
- Ne jamais transmettre d'informations sensibles par email (mot de passe, numéro de carte bancaire, etc.).
- Signaler immédiatement tout email suspect à l'équipe informatique.
- Vérifier que les emails de l'entreprise sont protégés par **SPF, DKIM et DMARC**.

## 4. Bonnes pratiques générales

- Verrouiller sa session dès qu'on quitte son poste, même pour quelques minutes.
- Ne jamais laisser une session ouverte en fin de journée.
- Ne pas installer de logiciels sans autorisation.
- Mettre à jour régulièrement son système et ses logiciels.
- Ne pas connecter de clé USB ou disque dur externe non vérifié.

- Utiliser uniquement les outils validés par l'entreprise pour le télétravail (VPN, RDP sécurisé).

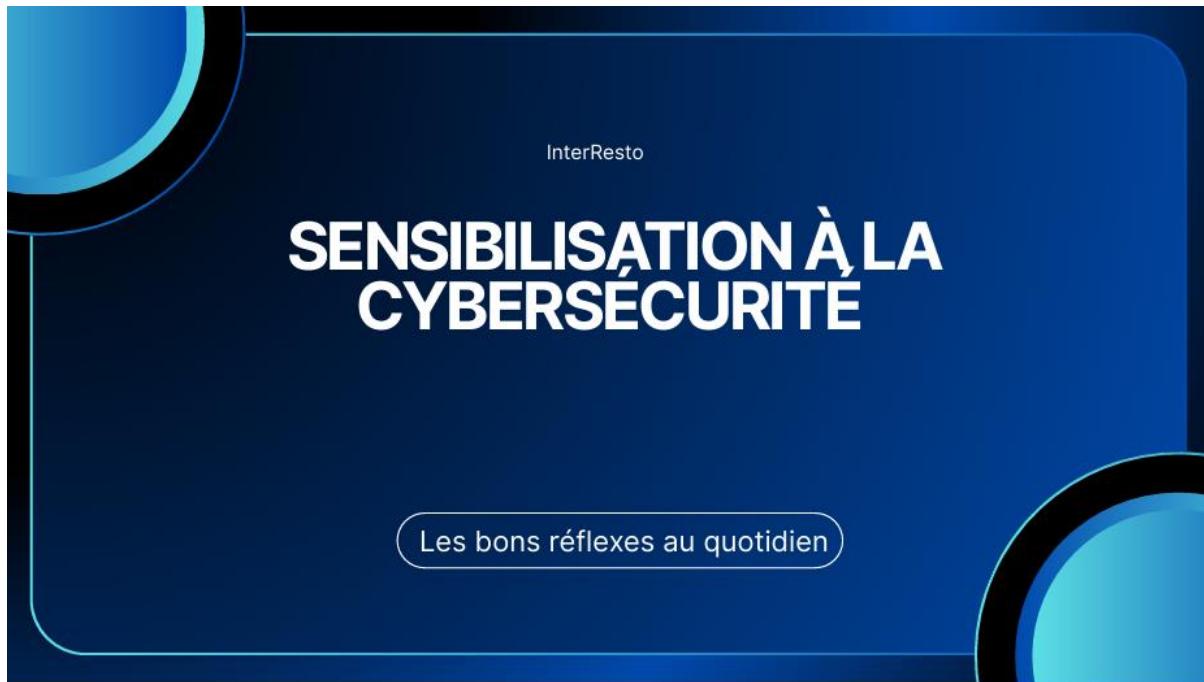
## 5. Télétravail et accès distant

- Utiliser uniquement les solutions sécurisées mises en place par l'entreprise (VPN, bureau à distance).
- Ne jamais accéder aux données de l'entreprise depuis un réseau Wi-Fi public.
- Verrouiller son ordinateur personnel si utilisé pour le travail.
- Respecter les mêmes règles de sécurité qu'au bureau.

## 6. Engagement

Chaque collaborateur s'engage à respecter cette charte et à contribuer activement à la sécurité de l'entreprise. En cas de doute ou de problème, il est tenu de contacter l'équipe informatique.

## Annexe D : PowerPoint de sensibilisation



# POURQUOI LA CYBERSÉCURITÉ ?

- 1 clic peut créer un problème sérieux 
- Les données de l'entreprise sont sensibles
- La cybersécurité dépend de chacun de nous

“Un geste simple peut protéger toute l'entreprise.”



## MOT DE PASSE

-  Mot de passe long et complexe
-  Ne pas réutiliser le même mot de passe
-  Activer la double authentification (MFA)

“Un mot de passe fort = données protégées.”



# EMAILS ET PHISHING

"Chaque email peut être une menace."

- Méfiez-vous des liens et pièces jointes inconnus
- Vérifiez l'expéditeur avant de cliquer
- En cas de doute → ne pas cliquer, signaler !

Phishing   Ransomware   Malware   DDoS Attacks



# POSTES DE TRAVAIL

"Un poste sécurisé protège vos données."



- Verrouillez votre session avant de quitter le poste
- Ne laissez pas d'informations sensibles sur le bureau
- Faites les mises à jour quand demandées

# SMARTPHONES ET WI-FI

“Un smartphone sécurisé protège aussi l’entreprise.”



- Connectez-vous uniquement aux réseaux de confiance
- Ne partagez pas votre téléphone pro
- Désactivez Bluetooth quand inutile

## CAS INTERRESTO

- Sessions Windows laissées ouvertes ✗
- Mot de passe faible ✗
- Pas encore de sensibilisation ✗

“Chacun peut améliorer la sécurité dès aujourd’hui.”



## À RETENIR!

### CE QU'IL FAUT RETENIR

- Mot de passe fort + MFA = meilleure protection
- Attention aux emails = éviter les risques
- Verrouiller sa session = protéger les données

“La cybersécurité commence par vous.”

### PETIT QCM D'AUTO-EVALUATION

Vrai/Faux : On peut utiliser le même mot de passe partout

Quel raccourci pour verrouiller un poste Windows ?

Vrai/Faux : Il est sûr d'ouvrir toutes les pièces jointes

Vrai/Faux : Le Wi-Fi public est sécurisé pour le travail

Vrai/Faux : La double authentification renforce la sécurité