ABAX INFO
SERVICES INFORMATIQUES

Rapport

Audit simple de l'environnement informatique

1. Constat actuel

Environnement de travail

- Poste unique à usage personnel et professionnel (multiutilisateur).
- PC sous Windows 10 Pro 22H2.
- Pas antivirus de nouvelle génération (EDR/XDR).
- Pare-feu public activé par défaut.
- Pas de sauvegarde mise en place.
- Disque dur non chiffré.
- Travail nomade

Navigateurs et accès

- Edge : mots de passe enregistrés, synchronisation avec compte Microsoft personnel et professionnel.
- Chrome : profils multiples (pro et client), mots de passe enregistrés.
- Sessions TSE configurées directement par le client, sans supervision ni contrôle.
- Google Drive utilisé comme espace de stockage/synchronisation (PC + smartphone Android) → pas de garantie de sauvegarde.
- Authentification à deux facteurs (2FA) active sur Google et Microsoft.

Prestataires externes

- Adobe : usage limité aux PDF, transfert par courriel sans suppression sur le stockage.
- Biim Com : gestion du site internet, domaine et messagerie.
- Microsoft (perso) : comptes utilisés à la fois pour le privé et le professionnel.

2. Besoins exprimés

- Centraliser les données.
- Simplifier les accès.

- Sécuriser les accès et les données.

3. Problèmes et frustrations

- Fonctionnalités limitées de la messagerie adlgestion vs Hotmail (ex. : envoi différé).
- Réception de messages en doublon (adlgestion et Hotmail).
- Accès TSE non fluide et présentant des risques de sécurité.

4. Analyse des risques

- **Mélange usage personnel et professionnel**
  → Les données de l'entreprise se retrouvent mélangées avec les données privées. En cas de mauvaise manipulation ou d'attaque, cela peut entraîner une **fuite d'informations sensibles**.
- **Absence de protection avancée (EDR/XDR)**
  → L'ordinateur n'est protégé que par un antivirus de base. Cela laisse la porte ouverte aux **virus modernes, ransomwares et cyberattaques sophistiquées**.
- **Pas de sauvegarde fiable**
  → En cas de panne, de vol ou d'attaque informatique, **les données peuvent être perdues définitivement**.
- **Mots de passe enregistrés dans les navigateurs**
  → Si l'ordinateur est compromis, les identifiants enregistrés sont facilement accessibles aux pirates, ce qui peut mener à des **intrusions dans les comptes professionnels et personnels**.
- **Absence de chiffrement du disque dur**
  → En cas de vol ou de perte du PC, toutes les données qu'il contient sont **immédiatement lisibles** par un tiers.
- **Utilisation d'un cloud grand public (Google Drive) sans supervision**
  → Les fichiers de l'entreprise sont stockés sur un outil qui n'offre **ni contrôle de sécurité, ni garantie de pérennité**, ce qui expose les données à des risques de perte ou de fuite.
- **Travail nomade sans VPN**
  → Lorsque vous travaillez à distance (chez elle, en déplacement, dans un café ou un hôtel), vous ne connaissez pas le niveau de protection du réseau sur lequel vous vous trouvez.

5. Recommandations ABAX INFO

Sécurité du poste de travail

- Déployer une solution de protection nouvelle génération (EDR).
- Activer le chiffrement BitLocker sur le disque dur.
- Configurer une sauvegarde automatique (locale + cloud).
- Garder le poste à jour avec supervision.

Gestion des accès

- Séparer usage personnel et professionnel (navigateur, comptes Microsoft/Google). L'idéal serait deux sessions distinctes (perso et pro) sur l'ordinateur.
- Interdire le stockage des mots de passe dans les navigateurs → utiliser un gestionnaire de mot de passe.
- Maintenir et renforcer l'usage du 2FA sur tous les services critiques.

Collaboration et données

- Centraliser les données sur Microsoft 365 Business Premium (OneDrive Entreprise + SharePoint).
- Migrer la messagerie sur Exchange Online avec gestion du domaine via Microsoft.
- Mettre en place un plan de gouvernance cloud (droits d'accès, partage sécurisé, audit régulier).

Accès distant

- Mettre en place un VPN lorsque vous vous connectez sur les environnements de vos clients ou en déplacement.

Prestataires externes

Vous êtes propriétaire de votre nom de domaine, mais le contrat établi avec votre webmaster en limite l'usage.
Ce contrat a débuté le **30/11/2023** pour une durée de **48 mois irrévocable**, et prendra fin le **30/11/2027**.

Toutes évolution du site devra passer par BIIM jusque-là. Vous avez toutefois la possibilité d'exiger la sécurité du site. De plus votre contrat vous permet une modification (1 page) par mois.

⚠️ Attention : si vous ne stoppez pas dès maintenant le renouvellement, le contrat sera automatiquement prolongé de **24 mois supplémentaires**.

Nous avons la possibilité de mettre en place un **portail collaboratif Microsoft**. Toutefois, la **gestion des zones DNS** restera sous la responsabilité de **BIIM**.
En cas de refus ou de blocage de leur part, il est également envisageable de **choisir une nouvelle extension** (par exemple : *adlgestion.com*) pour retrouver une liberté complète de gestion.

6. Plan d'action proposé

Étape	Action	Solution ABAX INFO	Priorité
1	Sécurisation du poste	EDR + BitLocker + Sdauvegarde	Haute
2	Gestion des mots de passe	Keeper Security	Haute
4	Migration messagerie et Centralisation des données	SharePoint + OneDrive Entreprise	Haute
5	Accès distant	VPN	Moyenne
6	Gouvernance	Sécuriser, optimiser, accompagner	Continue

Conclusion

L'environnement actuel présente des risques élevés de fuite ou de perte de données. Nous recommandons une mise en conformité progressive mais priorisée, avec une centralisation sous Microsoft 365, une sécurisation des postes et une gestion rigoureuse des accès.