Introduction

Le présent rapport fait état d’un projet de recensement exhaustif du patrimoine informatique de l’entreprise Digital Bureautique Solution (DBS). Mené dans le cadre de ma formation en BTS Services Informatiques aux Organisations (SISR), ce projet vise à inventorier l’ensemble des équipements et ressources informatiques de l’entreprise, évaluer leur conformité aux standards de sécurité et de performance, et proposer des améliorations en matière de gestion et de continuité des services informatiques. Le recensement s’appuie sur des référentiels de gestion d’actifs basés sur les normes ITIL, et a été réalisé en utilisant des outils dédiés pour garantir une gestion centralisée, fiable et à jour.

Les objectifs principaux étaient de :

- Répertorier tous les équipements informatiques et logiciels utilisés par DBS.

- Identifier les éventuels risques en matière de sécurité et proposer des recommandations pour une meilleure conformité.

- Optimiser les cycles de sauvegarde et vérifier les procédures de continuité de service afin de garantir la résilience et la disponibilité des ressources.

1. Méthodologie du recensement

Le recensement a été structuré en plusieurs étapes pour garantir une couverture complète et une collecte de données exhaustive. Les étapes comprennent la planification, la collecte et la structuration des données, et enfin l’analyse des données recueillies.

Planification et préparation

Pour mener à bien le recensement, une réunion préparatoire a été tenue avec moi-même afin de définir les périmètres d’analyse et d’identifier les zones prioritaires. Une liste de vérification a été établie, couvrant chaque type de matériel et de logiciel à inventorier, ainsi que les droits d’accès associés et les processus de sauvegarde.

Collecte et structuration des données

Chaque ressource a été identifiée, classée, et documentée dans un logiciel de gestion de patrimoine informatique (Userdiag). Cette étape a permis de collecter des informations précises sur chaque équipement, incluant :

- La nature de l’équipement (poste de travail),

- Le modèle et le numéro de série,

- L'utilisateur principal et ses autorisations d'accès sont détaillés en annexe,

- L’état de fonctionnement et la localisation.

Analyse et évaluation des risques

Les équipements recensés ont été analysés en fonction de leur conformité aux standards de sécurité et de performance. Les droits d’accès ont été vérifiés pour s’assurer qu’ils correspondaient aux besoins réels et aux responsabilités des utilisateurs. Enfin, l’efficacité des procédures de sauvegarde et les mécanismes de continuité de service ont été examinés pour détecter toute lacune éventuelle.

2. Inventaire des actifs informatiques

L’inventaire a permis de dresser une cartographie détaillée des actifs informatiques de DBS. Voici les principaux éléments identifiés :

Postes de travail et périphériques : L’entreprise dispose de 7 postes de travail répartis entre les services administratifs, techniques, et de vente. Chaque poste a été identifié par son modèle, son système d’exploitation, et ses principales applications installées. Les périphériques associés, tels que les imprimantes, ont également été inventoriés, ainsi que leur état de fonctionnement et leur maintenance.

Serveurs : DBS possède 1 serveur principal qui hébergent les applications métier et les données critiques. Il est dédié aux applications internes et aux sauvegardes.

Équipements réseaux : Les routeurs, switchs et points d’accès Wi-Fi de l’entreprise ont également été recensés. Les configurations réseau ont été examinées pour identifier les points de vulnérabilité et assurer une connexion stable et sécurisée.

Logiciels : Une liste exhaustive des logiciels utilisés dans l’entreprise a été établie, incluant les licences associées. Parmi eux, des logiciels de gestion d’entreprise, des outils de sécurité et des applications spécifiques pour la bureautique.

3. Analyse des manquements en matière de sécurité

L’analyse de l’inventaire a permis de relever plusieurs lacunes en matière de sécurité et de conformité. Voici les principaux points relevés :

Droits d’accès et habilitations : Certains comptes utilisateurs avaient des droits d’accès supérieurs aux besoins réels de leur titulaire. Par exemple, des employés des services administratifs possédaient des autorisations d’accès aux serveurs qui n’étaient pas nécessaires pour leurs tâches quotidiennes. Ce manque de contrôle sur les habilitations représente un risque potentiel de fuite de données ou d’erreurs critiques.

Mises à jour et correctifs de sécurité : Plusieurs postes de travail et serveurs n’avaient pas appliqué les derniers correctifs de sécurité, laissant les équipements exposés à des failles connues. Il a été observé que le processus de mise à jour manuelle rendait difficile une gestion efficace des correctifs.

Sauvegardes et continuité de service : Les sauvegardes sont effectuées sur une base hebdomadaire, mais sans vérification systématique de l’intégrité des fichiers sauvegardés. De plus, aucun test de restauration n’avait été réalisé, ce qui rend la continuité de service incertaine en cas de sinistre.

Politique de mots de passe : La politique de mots de passe de DBS n’est pas en adéquation avec les standards de sécurité actuels. Plusieurs utilisateurs avaient des mots de passe simples, facilement devinables, et aucun système de double authentification n’était mis en place pour les accès critiques.

4. Recommandations pour la mise en conformité

Pour corriger les manquements identifiés et améliorer la sécurité du parc informatique, plusieurs recommandations sont proposées :

Révision des droits d’accès : Mettre en place un système de gestion des habilitations plus strict et limiter les droits d’accès des utilisateurs en fonction de leurs responsabilités. Ce contrôle doit être révisé régulièrement pour ajuster les autorisations en cas de changement de fonction ou de départ de l’entreprise.

Automatisation des mises à jour : Utiliser une solution de gestion des correctifs automatisée pour assurer que tous les systèmes reçoivent les mises à jour de sécurité nécessaires. Cela permettra de réduire les vulnérabilités et d’assurer la sécurité des données.

Renforcement des politiques de sauvegarde : Les sauvegardes doivent être effectuées quotidiennement pour réduire la perte de données en cas de panne. Des tests de restauration réguliers sont également essentiels pour garantir la continuité du service et la fiabilité des copies de sauvegarde.

Amélioration de la politique de mots de passe : Mettre en place une politique de mots de passe renforcée, exigeant des combinaisons complexes et un changement régulier des identifiants. La mise en place d’une double authentification pour les accès critiques est également fortement recommandée.

5. Optimisation des cycles de sauvegarde et de continuité de service

Pour garantir une résilience optimale et la continuité de service, DBS devrait envisager les améliorations suivantes :

Sauvegardes incrémentales : Au lieu de sauvegardes complètes hebdomadaires, la mise en place de sauvegardes incrémentales quotidiennes permettrait de réduire les risques de perte de données et de minimiser l'impact sur les ressources.

Solution de récupération d'urgence : Un plan de reprise d’activité devrait être élaboré pour assurer la continuité des opérations en cas de sinistre. Ce plan inclurait des procédures de redémarrage pour chaque composant critique et des tests de simulation.

Surveillance en temps réel : L’utilisation d’un système de surveillance en temps réel permettrait d’anticiper les problèmes avant qu’ils n’affectent le service. Une alerte en cas de défaillance détectée dans le réseau ou sur les serveurs permettrait de réagir immédiatement.

Conclusion

Le recensement du parc informatique de DBS a permis de fournir une vue d’ensemble détaillée des actifs numériques et de détecter des zones de risques en matière de sécurité et de continuité de service. En suivant les recommandations de ce rapport, DBS pourra améliorer la sécurité de son infrastructure, assurer une gestion rigoureuse des droits d’accès, et garantir la disponibilité continue des services. Une mise en place progressive des améliorations et un suivi régulier seront essentiels pour adapter la gestion des ressources aux besoins évolutifs de l’entreprise.