ABAX INFO
SERVICES INFORMATIQUES

Rapport

Audit simple de l'environnement informatique

Constats

- Il existe une exposition directe à l'internet car il n'y a pas de pare-feu dédié. C'est la box Swisscom qui opère seule.
- Le Wi-Fi est effectué via une borne Apple grand public qui ne dispose pas de sécurité robuste ni séparation des réseaux.
- Les utilisateurs sont administrateur local de leur poste.
- Les antivirus sont absents ou gratuits.
- Le Windows Server 2012 est obsolète et Il existe une hétérogénéité de postes Win10/Win11 avec des systèmes hors suivi de l'éditeur.
- Il existe une dépendance critique mal isolées car le VPN OpenVPN est hébergé sur le Synology qui fait aussi la sauvegarde. Cela crée un risque de compromission croisée.

Risque

La société Burgener SA est expose à un risque d'incident majeur : ransomware / fuite de données / indispo en raison des constats énoncés.

1. Ransomware avec chiffrement global (serveur fichiers, Synology, postes) via un poste admin non protégé.
2. Intrusion externe (absence de firewall NGFW/IPS), pivot vers AD et exfiltration de données.
3. Interruption d'activité (panne NAS ou serveur 2012), restauration lente/incertaine faute de PRA testé.
4. Fuite de données via Wi-Fi de production utilisée par des tiers ou via OpenVPN/NAS.

Priorités

- Immédiat (0–1 mois)
    - Déployer des antivirus de dernière génération.
    - Superviser les mises à jour et des vulnérabilités.
    - Appliquer les correctifs de vulnérabilités.
    - Forcer le MFA pour tous les accès distants et pour M365.
    - Retirer les droits administrateurs des comtes locaux.
    - Activer le BitLocker (TPM) et le Secure Boot des postes.

- Court terme (1–3 mois)
    - Mettre en place un pare-feu et activer le VPN via ce dernier (Le NAS ne doit faire que la sauvegarde).
    - Créer des VLANs : Production, Sauvegarde, Invités, VoIP pour cloisonner le NAS de sauvegarde (VLAN Sauvegarde, comptes dédiés, pas en AD admin),
    - Tester la restauration des données.
    - Mettre en place une stratégie 3-2-1 : 3 copies, 2 supports, 1 hors site (cloud immuable/S3 WORM).
    - Préparer des routines d'arrivée et de départ de collaborateurs (comptes, accès, équipements).
    - Mettre en place des visites préventives
    - Remplacer la borne Apple par une borne professionnel. Créer SSID invité isolé.
    - Contrôler et superviser la sauvegarde.

- Moyen terme (3–6 mois)
    - Plan PRA (scénarios panne) RPO/RTO documentés.
    - Charte informatique et campagne de sensibilisation phishing (1 à 2 fois/an).

- Moyen/long terme (6-12 mois)
    - Inventorier rôles et dépendances du Windows Server 2012 (DHCP, AD, fichiers, applis).
    - Nouveau serveur Windows Server 2022 (ou VM sur hôte récent) et migrer AD/DNS/DHCP.