CONSTATS TYPES PAR SEGMENT

Document de référence pour l'analyse des diagnostics

Version 1.0 **Siba KOIVOGUI** **OPSIE M2 Lyon 2**

Ce document recense les vulnérabilités et constats les plus fréquemment observés dans chaque segment cible. Il sert de référence pour : - Préparer les questions d'entretien - Orienter l'analyse des grilles d'audit - Formuler des recommandations pertinentes - Enrichir l'analyse critique du rapport

SOURCES : - ANSSI, Panorama de la cybermenace 2023 - ANSSI, Guide cybersécurité TPE/PME 13 questions, 2021 - CNIL, Rapport d'activité 2023 - ENISA, Threat Landscape 2023 - Cybermalveillance.gouv.fr, Rapport d'activité 2023

SEGMENT 1 — TPE-PME

PROFIL TYPE

- 0 à 250 salariés
- Pas de RSSI ni d'équipe IT dédiée
- Prestataire informatique externe (souvent 1 seul)
- Budget IT < 5 000 €/an
- Dirigeant = décideur unique sur toutes les questions IT

VULNÉRABILITÉS LES PLUS FRÉQUENTES

1. MOTS DE PASSE FAIBLES ET PARTAGÉS - Utilisation du même mot de passe pour tous les services - Mots de passe notés sur post-it ou fichier Excel non protégé - Pas de renouvellement périodique - Comptes partagés entre plusieurs employés Risque : accès non autorisé, propagation rapide en cas de compromission Source : ANSSI — 80 % des incidents impliquent des credentials compromis

2. ABSENCE DE SAUVEGARDES FIABLES - Sauvegardes sur le même réseau que les données (inefficace contre ransomware) - Sauvegardes jamais testées (restauration non vérifiée) - Pas

de sauvegarde hors site ou cloud - Fréquence insuffisante (hebdomadaire au lieu de quotidienne) Risque : perte totale de données en cas de ransomware ou sinistre

3. LOGICIELS NON MIS À JOUR - Windows / macOS en version obsolète - Logiciels métier non patchés depuis des mois/années - Antivirus expiré ou absent Risque : exploitation de vulnérabilités connues et corrigées

4. RGPD NON APPLIQUÉ - Registre des traitements inexistant (obligation légale) - Pas de politique de confidentialité sur le site web - Consentement cookies absent ou non conforme - Données clients stockées sans sécurisation (fichiers Excel partagés) Risque : sanction CNIL, amende jusqu'à 4 % du CA mondial

5. PHISHING — PREMIER VECTEUR D'ATTAQUE - Employés non sensibilisés à la détection d'emails frauduleux - Pas de filtre anti-spam efficace - Ouverture de pièces jointes malveillantes Risque : compromission du SI, ransomware, fraude au président Source : cybermalveillance.gouv.fr — phishing = 1er incident déclaré

6. PAS DE PLAN DE CONTINUITÉ - Aucune procédure documentée en cas de cyberattaque - Pas de contacts d'urgence connus (prestataire, ANSSI, assurance) - RTO (temps de reprise) non défini Risque : arrêt d'activité prolongé, perte clients

7. ACCÈS DISTANTS NON SÉCURISÉS - Télétravail via connexion personnelle sans VPN - Accès aux données via outils non professionnels (Google Drive personnel...) Risque : interception de données, accès non autorisé

RECOMMANDATIONS STANDARD TPE-PME

Court terme (0-3 mois, coût faible) : - Gestionnaire de mots de passe (Bitwarden gratuit, 1Password ~3€/mois) - Activation MFA sur tous les comptes critiques (email, banque, logiciels) - Plan de sauvegarde 3-2-1 (3 copies, 2 supports, 1 hors site) - Mise à jour immédiate de tous les systèmes - Registre RGPD simplifié (modèle CNIL gratuit)

Moyen terme (3-6 mois) : - Formation anti-phishing des employés (1 demi-journée) - Charte informatique - Procédure de gestion des incidents (1 page suffit) - Audit du prestataire informatique actuel

Long terme (6-12 mois) : - PCA simplifié - Assurance cyber - Audit annuel

SEGMENT 2 — COLLECTIVITÉS TERRITORIALES

PROFIL TYPE

- Communes, EPCI, départements, régions
- DSI mutualisée ou prestataire unique
- Données sensibles : état civil, urbanisme, données des administrés
- Contrainte NIS2 depuis 2024
- Prise de décision longue (processus administratif)
- Budget IT insuffisant vs. enjeux

VULNÉRABILITÉS LES PLUS FRÉQUENTES

1. DÉPENDANCE À UN PRESTATAIRE UNIQUE - Un seul prestataire IT gère tout le SI - Pas de SLA formalisé (délais d'intervention non garantis) - Pas de plan B si le prestataire fait défaut Risque : paralysie totale en cas de défaillance du prestataire Source : ANSSI — situation observée dans de nombreuses collectivités victimes

2. RANSOMWARE — VECTEUR PRINCIPAL (+80 % ANSSI 2023) - Sauvegardes sur le même réseau (chiffrées en même temps que les données) - Pas de segmentation réseau - Accès RDP (bureau à distance) exposé sur Internet sans protection Risque : paralysie complète des services, coût moyen > 500 000 € pour une collectivité de taille moyenne Source : ANSSI, Panorama de la cybermenace 2023

3. NON-CONFORMITÉ NIS2 - Méconnaissance de la directive par les élus et la direction - Pas de registre des risques - Pas de procédure de notification d'incident (obligation < 24h) - Sécurité de la chaîne d'approvisionnement non évaluée Risque : non-conformité réglementaire, responsabilité des élus

4. COMPTES ADMINISTRATEURS MAL GÉRÉS - Comptes à privilèges élevés utilisés pour des tâches courantes - Comptes partagés entre agents - Comptes d'anciens agents non désactivés Risque : propagation rapide d'une attaque, accès non autorisé

5. MESSAGERIE ET DONNÉES NON CHIFFRÉES - Échanges de données personnelles des administrés par email non chiffré - Documents d'état civil partagés via des canaux non sécurisés Risque : violation RGPD, fuite de données sensibles

6. MANQUE DE SENSIBILISATION DES AGENTS - Agents non formés à la cybersécurité - Pas de charte informatique ou charte non appliquée - Utilisation d'appareils personnels pour des tâches professionnelles Risque : phishing, ingénierie sociale, fuite de données

7. ABSENCE DE GOUVERNANCE CYBER - Pas de référent cybersécurité désigné - Absence de politique de sécurité SI formalisée - Pas de revue régulière des accès Risque : absence de pilotage, réponse aux incidents chaotique

RECOMMANDATIONS STANDARD COLLECTIVITÉS

Court terme : - Désigner un référent cybersécurité (même partiel) - Sauvegardes hors ligne testées mensuellement - Désactiver les comptes des agents ayant quitté la collectivité - Sensibilisation des agents (1 session/an minimum) - Inventaire des systèmes critiques

Moyen terme : - Segmentation réseau (séparation services en ligne / réseau interne) - Procédure de notification d'incident NIS2 (< 24h) - Contrat de prestation IT avec SLA formalisés - Plan de continuité des services essentiels

Long terme : - Audit annuel de sécurité - Mutualisation avec d'autres collectivités (GIP...) - Mise en conformité NIS2 complète

SEGMENT 3 — ASSOCIATIONS

PROFIL TYPE

- Associations employeuses (secteur social, santé, sport, culture...)
- Données sensibles : bénéficiaires (santé, situation sociale), adhérents
- Budget IT quasi-nul
- Bénévoles utilisent leurs équipements personnels
- Pas de compétences informatiques internes
- Responsable = souvent bénévole non technicien

VULNÉRABILITÉS LES PLUS FRÉQUENTES

1. ABSENCE DE REGISTRE RGPD - Aucun recensement des données traitées - Pas de base légale identifiée pour les traitements - Données de santé des bénéficiaires traitées sans encadrement Risque : violation RGPD, amende CNIL, perte de confiance des bénéficiaires Note : les associations traitant des données de santé ou données sensibles ont des obligations RGPD renforcées

2. PARTAGE DE DONNÉES PAR EMAIL NON CHIFFRÉ - Dossiers de bénéficiaires envoyés par Gmail/Hotmail - Partage de fichiers via WhatsApp (données hors UE) - Documents partagés

via Google Drive personnel sans contrôle d'accès Risque : fuite de données personnelles et sensibles

3. ÉQUIPEMENTS PERSONNELS DES BÉNÉVOLES - Bénévoles utilisent leur ordinateur/ téléphone personnel - Aucun contrôle de la sécurité de ces équipements - Données de l'association stockées sur des appareils privés Risque : perte de données si appareil perdu/ volé, contamination malware

4. PAS DE GESTION DES ACCÈS - Mêmes identifiants partagés entre tous les bénévoles - Pas de distinction des droits selon le rôle - Accès aux données maintenus après départ d'un bénévole Risque : accès non autorisé aux données, impossibilité d'audit

5. SITE WEB NON CONFORME - Formulaires de contact sans mentions RGPD - Pas de politique de confidentialité - Cookies non gérés (Google Analytics non configuré) Risque : non-conformité RGPD, mise en demeure CNIL

6. AUCUNE SENSIBILISATION AUX CYBERRISQUES - Bénévoles ignorent les risques de phishing et d'hameçonnage - Pas de procédure en cas d'incident - Dirigeants associatifs non sensibilisés Risque : incident par manque de vigilance élémentaire

7. DONNÉES FINANCIÈRES MAL PROTÉGÉES - Fichiers comptables sur disque dur non sauvegardé - Coordonnées bancaires des adhérents peu protégées Risque : fraude, perte de données financières

RECOMMANDATIONS STANDARD ASSOCIATIONS

Court terme (priorité absolue, coût quasi-nul) : - Registre RGPD simplifié (modèle CNIL gratuit, 2h de travail) - Mentions légales et politique de confidentialité sur le site (modèles gratuits) - Espace de partage sécurisé (Nextcloud, Drive professionnel) - MDP différents par service et gestionnaire de mots de passe

Moyen terme : - Sensibilisation des bénévoles (1h suffit) - Charte informatique pour bénévoles - Procédure de départ d'un bénévole (suppression des accès) - Sauvegarde des données essentielles

Long terme : - Équipement professionnel partagé (un ordinateur dédié aux données sensibles) - Mise en conformité RGPD complète avec DPO bénévole si possible

TABLEAU DE COMPARAISON DES NIVEAUX DE MATURITÉ OBSERVÉS

Domaine	TPE-PME	Collectivités	Associations
Gouvernance cyber	Faible	Faible	Très faible
RGPD	Faible	Modéré	Très faible
Sauvegardes	Faible	Faible	Très faible
Gestion des accès	Faible	Modéré	Très faible
Sensibilisation	Très faible	Faible	Très faible
Plan de continuité	Très faible	Faible	Inexistant
Sécurité technique	Faible	Modéré	Très faible
Conformité NIS2	N/A*	Très faible	N/A*
Conformité DORA	Très faible*	N/A	N/A

(*) selon le secteur et les clients de la structure

SOURCES CITABLES DANS LE RAPPORT : - ANSSI, Panorama de la cybermenace 2023 — p. 12-18 - Cybermalveillance.gouv.fr, Rapport d'activité 2023 - CNIL, Rapport d'activité 2023 — sanctions et mises en demeure - ENISA, Threat Landscape 2023 — SME chapter - Directive (UE) 2022/2555 — NIS2 - Règlement (UE) 2022/2554 — DORA