ALTIORIS Aero Conseil
Thierry ROUSSEL – Expert Qualité
Auditeur certifié ISO 9001 IRCA
Tel. : 06.63.75.84.15
https://altioris-aero.fr

Guide pratique en matière de Cybersécurité

Objectif

Protéger les systèmes d'information, limiter les risques d'attaques (rançongiciels, espionnage, vols de données) et renforcer la confiance des clients, partenaires et autorités.

Bonnes pratiques essentielles

- **Mots de passe robustes** : uniques, longs (12+ caractères), renouvelés régulièrement.
- **Mises à jour** : systèmes, logiciels, antivirus toujours à jour.
- **Sauvegardes** : régulières, testées, déconnectées du réseau (stockage externe / cloud sécurisé).
- **Contrôle des accès** : droits limités au strict nécessaire (principe du moindre privilège).
- **Cloisonnement réseau** : séparer postes utilisateurs, serveurs critiques, accès Internet.
- **Messagerie & navigation** : vigilance face aux liens et pièces jointes, utiliser les sites éditeurs officiels.
- **Nomadisme sécurisé** : protéger smartphones, tablettes, ordinateurs portables (chiffrement, VPN).
- **Séparation usages pro/perso** : pas de mélange sur ordinateurs, emails ou supports USB.
- **Prestataires & utilisateurs identifiés** : pas de comptes anonymes, gestion rigoureuse des arrivées/départs.
- **Sensibilisation du personnel** : formation régulière, charte informatique, réflexes à adopter.

Réagir en cas de cyberattaque

- **Isoler rapidement** les machines infectées.
- **Préserver les preuves** (ne pas réinitialiser trop vite).
- **Ne pas payer la rançon** (aucune garantie de récupération des données).
- **Activer le plan de réponse** (continuité d'activité, communication de crise).
- **Informer** : CNIL si données personnelles, clients/partenaires si impact direct.
- **Porter plainte** et demander l'appui d'experts (ANSSI, Cybermalveillance.gouv.fr).
- **Restaurer** à partir de sauvegardes saines.

🔑 Informations complémentaires

- **Les PME et ETI sont des cibles privilégiées** : elles détiennent des données précieuses (financières, clients, R&D) et sont souvent le maillon faible de la supply chain.
- **L'humain reste la première ligne de défense** : plus de 80 % des attaques réussies exploitent une erreur humaine (phishing, ouverture de pièce jointe, clic malveillant).
- **Le RGPD impose des obligations fortes** : notification des fuites de données personnelles à la CNIL et information des personnes concernées.
- **Investir dans la cybersécurité est créateur de valeur** : c'est un gage de fiabilité pour les clients, un argument commercial lors des appels d'offres, et un facteur de confiance pour les banques et investisseurs.
- **La préparation est clé** : disposer d'un plan de continuité d'activité (PCA) et d'un plan de reprise après sinistre (PRA) est indispensable pour limiter l'impact d'une attaque.

🚀 Bénéfices

- Réduction des risques d'arrêt d'activité et de pertes financières.
- Conformité réglementaire (RGPD, exigences clients).
- Valorisation de l'image et de la fiabilité de l'organisation.
- Avantage compétitif dans les appels d'offres.

👉 Ce guide est une **feuille de route pratique** pour toute entreprise (TPE, PME, ETI, grands groupes) souhaitant améliorer sa **maturité cyber** et assurer sa résilience numérique.

Pour aller plus loin contactez nous :

SASU ALTIORIS Aero Conseil – SIRET 988 012 399 00016