# LE GUIDE POUR LES TPE/PME

*Sécurisez votre système d'information*



Hexatel

# SOMMAIRE

*Sécurisez votre système d'information*


01 Pourquoi sécuriser votre SI ? *p3*

02 Les risques auxquels vous êtes exposés *p4*

03 Sécuriser les accès au réseau *p6*

04 Protéger le réseau d'entreprise *p7*

05 Protéger les postes et les serveurs *p8*

06 Sauvegarder pour assurer la continuité d'activité *p9*

07 Sensibiliser et former les équipes *p10*

08 Faire appel à un prestataire IT *p11*

# TPE/PME : POURQUOI SÉCURISER VOTRE SI* ?

Aujourd'hui, aucune entreprise n'est à l'abri d'une cyberattaque, quel que soit son secteur ou sa taille. Beaucoup de TPE et PME sous-estiment encore la nécessité de protéger leur système d'information, alors qu'elles sont désormais des cibles privilégiées en raison de protections souvent insuffisantes.

Une attaque peut entraîner des conséquences majeures : interruption d'activité, perte de données, pertes financières, atteinte à la réputation... Ce guide a pour objectif de vous fournir les clés essentielles pour sécuriser votre SI à travers des conseils simples, concrets et directement applicables.

## Quelques données chiffrées sur les TPE/PME

**58%**

des TPE/PME déclarent être faiblement protégées

**72%**



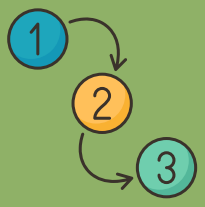
ne disposent d'aucun salarié dédié à la gestion du SI

**15%**

ont été touchées par un incident de cybersécurité durant les 12 derniers mois



**70%**




des entreprises ne disposent pas de procédure de réaction

*SI : système d'information

source : francenum.gouv

# LES RISQUES AUXQUELS VOUS ÊTES EXPOSÉS

La sécurité de votre système d'information repose avant tout sur une bonne connaissance des menaces qui pèsent sur votre entreprise. Parmi les plus courantes figurent le phishing, les ransomwares, les attaques par force brute, malware ou DDoS pouvant paralyser tout ou partie de votre infrastructure. D'autres menaces existent bien entendu, mais ces 5 risques représentent déjà des points de vigilance essentiels à maîtriser pour renforcer efficacement votre niveau de protection.

## 1 Phishing

Le phishing est l'attaque la plus courante contre les petites entreprises. Elle consiste à envoyer des e-mails, SMS ou messages instantanés usurpant l'identité d'un fournisseur, d'une banque ou même d'un collègue. L'objectif est de pousser un collaborateur à cliquer sur un lien piégé, télécharger une pièce jointe malveillante ou transmettre des informations sensibles (mot de passe, RIB, identifiants).

### Pourquoi c'est dangereux pour les TPE/PME ?

Les petites structures disposent souvent de moins de ressources pour former leurs équipes à la cybersécurité. Il suffit qu'un seul collaborateur se fasse piéger pour compromettre la messagerie, les accès cloud ou les données clients... Le risque est également amplifié par le fait que les tâches administratives et financières sont souvent concentrées sur une ou deux personnes, ce qui facilite la manipulation.

## 2 Ransomware

Il s'agit d'un logiciel malveillant qui a pour but de bloquer l'accès à vos fichiers ou à l'ensemble de votre système informatique. Pour récupérer vos accès les cybercriminels vous demande une somme d'argent qui peut être conséquente. Un message s'affiche sur votre écran pour vous avertir de l'attaque en vous demandant le paiement de la rançon.

### Pourquoi c'est critique pour les TPE/PME ?

Les TPE/PME n'ont pas toujours de sauvegardes ou de plan de reprise après sinistre. Résultat : une attaque peut entraîner l'arrêt total de l'activité pendant plusieurs jours ou une perte de données critique. Certaines entreprises n'arrivent jamais à s'en relever. Ces attaques ciblent assez souvent les TPE/PME car les systèmes sont moins sécurisés et plus faciles à pénétrer.

## 3 Force brute

Avec les attaques par force brute, Les cybercriminels testent automatiquement des milliers de combinaisons d'identifiants pour accéder aux comptes professionnels (messagerie, VPN, outils cloud). Ils utilisent souvent des bases d'identifiants volées à d'autres services, en pariant que les utilisateurs réutilisent leurs mots de passe.

### Pourquoi les TPE/PME sont vulnérables ?

Les TPE/PME sont particulièrement vulnérables car elles utilisent encore trop souvent des mots de passe simples, répétés ou peu renouvelés. Sans politiques de sécurité strictes ni authentification multifactorielle, leurs accès deviennent des cibles faciles pour les cybercriminels. Une attaque réussie peut également ouvrir la voie à une intrusion plus large.

## 4 Malware

Les malwares comprennent plusieurs familles : chevaux de Troie, spywares (logiciels espions), keyloggers (enregistreurs de frappe)... Ces logiciels s'installent à l'insu de l'utilisateur et permettent d'espionner, de voler des données, de prendre le contrôle d'un poste ou de préparer une attaque plus importante.

### Pourquoi c'est un risque majeur pour les TPE/PME

Les PME utilisent souvent des postes hétérogènes, parfois mal mis à jour ou sans solution de protection centralisée. Un malware peut rester actif longtemps sans être détecté, voler des informations sensibles (clients, contrats, devis) ou ouvrir une brèche permettant une future attaque, notamment un ransomware.

## 5 DDoS

Une attaque par déni de service distribué (DDoS) consiste à submerger un site web, un serveur ou une application d'un volume massif de requêtes, jusqu'à rendre le service indisponible.

### Pourquoi les TPE/PME sont vulnérables ?

Les petites entreprises disposent rarement d'infrastructures dimensionnées pour absorber un trafic anormal. Une attaque DDoS peut donc rapidement bloquer un site marchand, un portail client, un service de réservation, un standard téléphonique...

# SÉCURISER LES ACCÈS RÉSEAUX

**Objectif :** limiter l'accès aux systèmes et données uniquement aux personnes autorisées, et rendre l'usurpation d'identité difficile.

## 01 Politique de mots de passe

- **Longueur minimale :** 12 caractères.
- **Complexité recommandée :** mélange de lettres, chiffres et symboles.
- **Interdiction :** mot de passe simple, réutilisé, nom d'entreprise, date de naissance...
- **Changement régulier :** tous les 6 à 12 mois selon la sensibilité des accès.
- **Outils recommandés :** utiliser un gestionnaire de mots de passe

## 02 Authentification multi-facteur (MFA)

La MFA doit être obligatoire partout où elle est disponible car c'est l'une des mesures les plus efficaces pour réduire les risques de compromission de comptes. Vous pouvez la paramétrer sur :

- vos services d'emails professionnels,
- outils Cloud (CRM, ERP, applications comptables),
- votre console d'administration informatique...

## 03 Gestion des droits utilisateurs

- Appliquer **le principe du moindre privilège :** un utilisateur n'a accès qu'aux données dont il a réellement besoin.
- Créer des **rôles standardisés** (ex. : commercial, comptabilité, direction, technique...)
- Retirer immédiatement les accès au départ d'un salarié ou les ajuster en cas de changement de poste

# PROTÉGER LE RÉSEAU D'ENTREPRISE

**Objectif :** Empêcher les intrusions, limiter la propagation d'attaques et protéger les échanges.

## 01 Segmentation du réseau

Il est conseillé de **créer des réseaux séparés** pour vos différents publics ou usages car cela limite les dégâts en cas d'infection ou d'intrusion :

- Réseau bureautique
- Réseau invités
- Réseau production / machines industrielles
- Réseau administration...

## 02 Sécurisation du Wi-Fi

Voici les principales mesures à prendre pour diminuer la vulnérabilité de votre Wifi :

- Interdire l'usage d'un mot de passe unique pour tous.
- Imposer un réseau invité distinct pour les visiteurs et les appareils non maîtrisés.

## 03 Pare-feu et filtrage

- Mettre en place un pare-feu physique
- Bloquer les ports inutilisés
- Filtrer les sites malveillants (DNS filtré, proxy).

# PROTÉGER LES POSTES ET LES SERVEURS

**Objectif :** Limiter l'exposition aux logiciels malveillants et empêcher les attaques de se propager.

## 01 Mises à jour

Pour augmenter son niveau de sécurité, il est indispensable de **procéder à des mise à jour régulières** de ses différents services et équipements :

- Automatiser les mises à jour Windows / macOS.
- Mettre à jour les logiciels métier (compta, CRM…).
- Mettre à jour le firmware des routeurs, switchs et Wi-Fi.

## 02 Antivirus

Installez un outil antivirus professionnel disposant des fonctionnalités clés suivantes :

- Analyse en temps réel
- Confinement automatique d'un poste infecté
- Remontée d'alertes centralisée.

## 03 Bonnes pratiques sur les postes

- Verrouillage automatique après 5 minutes
- Interdiction d'installer des logiciels non validés
- Sauvegarde automatique des documents critiques
- Chiffrement du disque

# SAUVEGARDER POUR LA CONTINUITÉ D'ACTIVITÉ

**Objectif :** Être capable de récupérer ses données après un incident (panne, ransomware, erreur humaine).

## 01 La règle du 3-2-1

Une sauvegarde efficiente doit respecter la règle 3-2-1, c'est à dire :

- **3 copies** de chaque donnée
- sur **2 supports** différents
- dont **1 hors site**

## 02 Chiffrement

Les données des sauvegardes doivent impérativement être chiffrées, surtout s'il s'agit de sauvegardes externalisée. Cela permet de préserver la confidentialité des données sauvegardées.

## 03 Tests de restauration

Un plan de sauvegarde n'est fiable que si les restaurations de données fonctionnent réellement. Pour s'assurer de cela, il est recommandé d'effectuer des tests de restauration trimestriels.

# SENSIBILISER ET FORMER LES ÉQUIPES

**Objectif :** Créer une culture cybersécurité, car 80 % des incidents viennent d'une erreur humaine.

## 01 Pourquoi la sensibilisation est essentielle ?

- Les TPE/PME sont des cibles privilégiées pour les cyberattaquants.
- Les cyberattaques exploitent majoritairement des comportements humains
- Une équipe sensibilisée = un risque divisé par 5

## 02 Thèmes essentiels à aborder

- Phishing et reconnaissance des emails frauduleux
- Gestion sécurisée des mots de passe
- Protection des données sensibles
- Bonnes pratiques nomades (Wi-Fi public, USB, voyages...)
- Politique d'usage des appareils personnels (BOYD)

## 03 Exercices pratiques à mettre en place

- Simulations de phishing (faux mails frauduleux envoyés à vos collaborateurs)
- Quiz de sensibilisation mensuels ou trimestriels
- Ateliers de 30 minutes de formation aux bonnes pratiques

## 04 Documentation et charte informatique

**Rédiger une charte informatique** à faire signer par tous les salariés et accessible à tous au quotidien simplement.

# FAITES APPEL À UN PRESTATAIRE EXTERNE

La plupart des TPE/PME n'ont **pas de service informatique interne.** Par manque de temps, de budget ou de compétences, elles gèrent souvent elles-mêmes leur système d'information, en s'appuyant sur des outils de sécurité limités.

Mais les cybermenaces évoluent vite et ciblent de plus en plus les petites structures. Pour se protéger efficacement, il faut **du temps et des compétences spécialisées :** veille permanente, gestion des incidents, supervision du réseau, mises à jour de sécurité, sauvegardes, continuité d'activité...

Faire appel à un prestataire externe vous permet de bénéficier d'un **accompagnement professionnel,** adapté à votre entreprise. C'est **un investissement maîtrisé,** souvent moins coûteux qu'une gestion interne, et qui vous apporte un niveau de sécurité, de continuité et de sérénité bien supérieur.

## 6 bonnes raisons de choisir l'infogérance pour votre sécurité IT

- Une protection renforcée et constamment à jour
- Une supervision continue 24/7
- Un expertise que les TPE/PME ne peuvent pas toujours internaliser
- Des coûts maîtrisés et prévisibles
- Une meilleure continuité d'activité
- Plus de temps pour se concentrer sur son coeur de métier

Hexatel

## Un projet ? Une question ?

Nos équipes sont là pour vous accompagner à chaque étape de vos projets télécoms, réseaux et informatiques.

Contactez-nous sur notre site internet