CHECKLIST PREVENTION CONTRE LES RAMSONWARE POUR LES PME

Table des matières

SÉCURITÉ DES POSTES & SERVEURS

État	Action	Détail
☐	Mettre à jour tous les systèmes	OS, logiciels, navigateurs, serveurs, CMS
☐	Installer un antivirus/EDR	Avec protection en temps réel et détection comportementale
☐	Bloquer les macros Office par défaut	Empêcher les scripts malveillants dans Word/Excel
☐	Restreindre PowerShell et les scripts	Interdire l'usage à tout utilisateur non admin
☐	Désactiver les ports inutiles (RDP, SMB...)	Surtout RDP si exposé à Internet
☐	Segmenter le réseau interne	Éviter la propagation entre machines/serveurs

GESTION DES UTILISATEURS

État	Action	Détail
☐	Supprimer les comptes inutilisés	Réduire les portes d'entrée
☐	Appliquer le principe du moindre privilège	Aucun utilisateur ne doit être admin local
☐	Activer l'authentification à deux facteurs (2FA)	Au minimum pour les accès critiques (mails, VPN, cloud)
☐	Former les employés à la cybersécurité	1 fois/an : phishing, pièces jointes, alertes

SAUVEGARDES

État	Action	Détail
☐	Mettre en place la règle 3-2-1	3 copies, 2 supports différents, 1 hors-ligne
☐	Automatiser les sauvegardes régulières	Quotidiennes au minimum
☐	Tester les restaurations chaque trimestre	Simuler un crash et restaurer les données

DÉTECTION ET SURVEILLANCE

État	Action	Détail
☐	Mettre en place un système de supervision (EDR, logs)	Surveiller les comportements suspects
☐	Configurer des alertes de détection	Activité anormale : exécution massive, renommage, etc.
☐	Suivre les journaux d'événements	Recherches sur les comptes, accès, erreurs systèmes

PLAN DE RÉPONSE À INCIDENT

État	Action	Détail
☐	Rédiger un plan de réponse à incident	Qui fait quoi ? Quand ? Quelles actions techniques ?
☐	Définir un référent cyber sécurité	Interne ou externe
☐	Conserver une copie papier/USB du plan	Utilisable même en cas de panne générale
☐	Simuler un scénario d'attaque	Table-top ou exercice annuel

COMMUNICATION & PARTENAIRES

État	Action	Détail
☐	Prévoir un message de crise (externe & interne)	Gérer la communication sans paniquer
☐	Connaître les contacts utiles	RSSI, prestataire IT, assureur cyber, ANSSI
☐	Vérifier la couverture cyber-assurance	Vérifier clauses ransomware et pertes d'exploitation