MY TRUST PARTNER

Cybersecurite - Conformite - IA

Cybersecurite des PME : par ou commencer ?

10 actions prioritaires, auto-diagnostic et roadmap 90 jours

LIVRE BLANC MTP 2026

www.mytrustpartner.fr - contact@mytrustpartner.fr - +33 1 84 16 05 27

Sommaire

1. Le constat : les PME en premiere ligne

2. Les 10 actions prioritaires

3. Auto-diagnostic en 10 questions

4. Roadmap 90 jours

5. Ou se faire accompagner

1. Le constat : les PME en premiere ligne

Une cible privilegiee

43 % des cyberattaques visent les PME (rapport ANSSI 2025). Raisons : budget cyber limite, pas de RSSI, outils grand public, sensibilisation faible, chaine d'approvisionnement mal maitrisee. Cout moyen d'une attaque reussie pour une PME : 150 000 euros, avec 60 % des victimes fermees dans les 6 mois.

Les 5 menaces principales

Ransomware (chiffrement des donnees, demande de rancon), phishing (vol d'identifiants, fraude au president), compromission email (BEC), exploitation de vulnerabilites non patchees, fuite de donnees via sous-traitant. Toutes sont massivement automatisees : pas besoin d'etre vise pour etre victime.

2. Les 10 actions prioritaires

1. MFA partout

L'authentification multi-facteurs sur tous les comptes (email, VPN, admin, acces distants). Solutions : Microsoft Authenticator, Google Authenticator, cles FIDO2. Reduction de 99 % des attaques par vol d'identifiants. Cout : gratuit a quelques euros par mois.

2. Sauvegardes 3-2-1 testees

3 copies, 2 supports differents, 1 hors site deconnecte (immuable). Sauvegardes testees mensuellement (restauration complete). Protection contre le ransomware : les sauvegardes accessibles en ligne sont chiffrees par l'attaquant en meme temps que la prod.

3. Mises a jour automatiques

Politique de patch systematique : postes, serveurs, pare-feu, applications metiers. Objectif : 95 % des vulnerabilites connues patchees sous 30 jours. 72 h pour les vulnerabilites critiques. La majorite des ransomwares exploitent des failles publiees il y a plus de 6 mois.

4. EDR sur 100 % du parc

Les antivirus classiques ne suffisent plus. EDR = detection comportementale + reponse automatique (isolation machine compromise). Solutions entreprise : Microsoft Defender for Endpoint, CrowdStrike, SentinelOne. 5 a 8 euros par poste par mois.

5. Sensibilisation reguliere

Formation initiale + rappels trimestriels + tests de phishing mensuels. Ciblage specifique : dirigeants (CEO fraud), comptabilite (fraude au virement), RH (faux CV contenant du malware). Formateurs labellises SecNumEdu-FC recommandes.

6. Filtrage email avance

Configurer SPF, DKIM, DMARC sur vos domaines. Solution anti-spam de nouvelle generation (sandbox pour analyser les pieces jointes, detection des tentatives d'usurpation). Filtrage URL sur les liens cliques. Cout : 3 a 10 euros par utilisateur par mois.

7. Plan de reponse a incident

Document de 10 pages maximum : qui contacter (interne, externe, CERT), premiers gestes (deconnexion, preservation des preuves), communication (clients, partenaires, autorites), continuite d'activite. Teste une fois par an en exercice de crise.

8. Assurance cyber

Couverture des frais de remediation, pertes d'exploitation, rancons (quand legal), frais juridiques et notifications RGPD. Primes a partir de 2 000 euros par an pour une PME de 50 personnes. Conditionne a un niveau minimum de cyberhygiene (MFA, sauvegardes, EDR).

9. Audit annuel

Audit externe : test d'intrusion, revue de configuration, analyse des risques. Identifie les angles morts de l'interne. Budget : 8 a 15 kEUR pour une PME. Livrable : plan d'action priorise.

10. Nommer un responsable cyber

Interne (RSSI ou DSI avec mandat) ou externe (CISO as a Service). Responsable de la strategie, du reporting direction, de la conformite, de la coordination en cas d'incident. Meme a temps partiel, essentiel.

3. Auto-diagnostic en 10 questions

Score 0-3

MFA sur les comptes admin et distants ? Sauvegardes testees et deconnectees ? EDR deploye sur tous les postes ? Patch des vulnerabilites critiques sous 7 jours ? Formation cyber annuelle pour tous ? Plan de reponse a incident ecrit ? SPF/DKIM/DMARC configures ? Test d'intrusion dans les 12 derniers mois ? Assurance cyber souscrite ? Responsable cyber designe ? Comptez 1 point par Oui.

Interpretation

0-3 : niveau critique, exposition extreme, action immediate requise. 4-6 : niveau insuffisant, plan de remediation a lancer. 7-8 : niveau acceptable, restent des angles morts a couvrir. 9-10 : niveau tres bon, objectif d'excellence et certification.

4. Roadmap 90 jours

Jours 1 a 30 - Les fondamentaux

Activer MFA sur tous les comptes admin et email. Verifier sauvegardes (completes, testees, hors ligne). Deployer EDR sur 100 % du parc. Lancer une campagne de sensibilisation. Configurer SPF/DKIM/DMARC.

Jours 31 a 60 - La consolidation

Formation equipe IT, inventaire complet des assets, politique de mot de passe + gestionnaire (Bitwarden, 1Password), filtrage email avance, revue des acces (principe du moindre privilege).

Jours 61 a 90 - La maturite

Plan de reponse a incident ecrit et teste, test d'intrusion externe, souscription d'une assurance cyber, nomination formelle d'un responsable cyber, premier tableau de bord mensuel.

Budget type PME 50 personnes

15 000 a 30 000 euros la premiere annee (outils + formation + audit), 8 000 a 15 000 euros en recurrent. A mettre en rapport avec le cout moyen d'une cyberattaque : 150 000 euros.

5. Ou se faire accompagner

Les criteres d'un bon prestataire

Labellisation SecNumEdu-FC par l'ANSSI pour la formation. Qualifications PRIS/PDIS pour l'audit et la reponse a incident. Equipe en France. Experience PME (pas uniquement grands comptes). Tarifs transparents.

Notre accompagnement

My Trust Partner propose une offre dedicee PME : diagnostic 360 degres (2 jours), plan d'action chiffre, mise en oeuvre accompagnee, suivi mensuel. Formations labellisees ANSSI. Tarifs adaptes aux ETI et PME. Consultation initiale gratuite : contact@mytrustpartner.fr, 01 84 16 05 27.

My Trust Partner

Cybersecurite - Conformite - IA

Labellise SecNumEdu-FC par l'ANSSI sur l'ensemble de notre catalogue formation.

Contact

www.mytrustpartner.fr
contact@mytrustpartner.fr
+33 1 84 16 05 27