

CHECKLIST

Évaluer sa posture de sécurité

Trente questions pour situer votre maturité en une heure, sans outil

Cette checklist ne remplace pas un audit. Elle sert à autre chose : donner à un dirigeant ou à un responsable informatique une vision honnête de sa situation en une heure, et identifier les deux ou trois sujets qui méritent un vrai examen. Répondez par oui seulement si vous pouvez le prouver.

Gouvernance et pilotage

- ☐ Une personne est nommément responsable de la sécurité des systèmes d'information.
- ☐ Une analyse de risques existe, et elle a moins de deux ans.
- ☐ La direction générale examine le sujet sécurité au moins deux fois par an.
- ☐ Un budget sécurité est identifié, distinct du budget informatique courant.
- ☐ Les obligations réglementaires applicables sont écrites et à jour.

Connaissance du patrimoine

- ☐ L'inventaire des serveurs, postes et équipements réseau est tenu à jour.
- ☐ Les applications exposées sur Internet sont recensées, avec un responsable pour chacune.
- ☐ Les données sensibles sont identifiées et leur localisation est connue.
- ☐ Les prestataires ayant un accès au système d'information sont listés.
- ☐ Les systèmes en fin de support sont connus et font l'objet d'un plan.

Accès et identités

- ☐ L'authentification à plusieurs facteurs protège les accès distants.
- ☐ Elle protège aussi les comptes à privilèges et la messagerie.
- ☐ Les comptes d'administration sont distincts des comptes nominatifs courants.
- ☐ Le départ d'un collaborateur déclenche une révocation tracée des accès.
- ☐ Les droits sont revus périodiquement, pas seulement attribués.

Protection des postes et des échanges

- ☐ Une solution de détection et réponse (EDR) est déployée sur les postes et les serveurs.

- [] Ses alertes sont traitées par quelqu'un, y compris en dehors des heures ouvrées.
- [] La messagerie est protégée contre l'hameçonnage et l'usurpation d'expéditeur.
- [] Les enregistrements SPF, DKIM et DMARC sont configurés sur vos domaines.
- [] Les correctifs de sécurité critiques sont appliqués sous un délai défini.

Détection et réponse

- [] Les journaux des systèmes critiques sont centralisés et conservés.
- [] Quelqu'un les regarde — automatiquement ou humainement — en continu.
- [] Une procédure écrite décrit qui alerter en cas d'incident, à toute heure.
- [] Le délai de notification réglementaire applicable est connu de l'équipe.
- [] Un incident majeur a déjà été simulé au cours des douze derniers mois.

Résilience

- [] Les sauvegardes couvrent l'ensemble des données critiques.
- [] Une copie est isolée du réseau et hors de portée d'un chiffrement.
- [] Une restauration complète a été testée, pas seulement planifiée.
- [] Le délai de reprise acceptable est défini avec les métiers, par application.
- [] Un plan de continuité existe et désigne les décideurs en cas de crise.

Lire son résultat

Comptez vos réponses positives. En dessous de quinze, la priorité est la connaissance du patrimoine et la protection des accès : sécuriser sans cartographier revient à équiper au hasard. Entre quinze et vingt-quatre, la protection est en place mais la détection et la capacité de réponse sont souvent le maillon faible. Au-delà de vingt-quatre, l'enjeu se déplace vers la mesure et la démonstration : prouver dans le temps que le dispositif fonctionne.

Les questions auxquelles vous avez hésité à répondre sont les plus instructives. Une hésitation signale presque toujours une mesure existante mais non vérifiée — c'est-à-dire une mesure sur laquelle on ne peut pas compter le jour où elle compte.

Ce document a une vocation informative et ne constitue pas un conseil juridique. Pour situer votre exposition réelle et vos priorités, échangez avec un expert ASEVIO : www.asevio.com/contact