

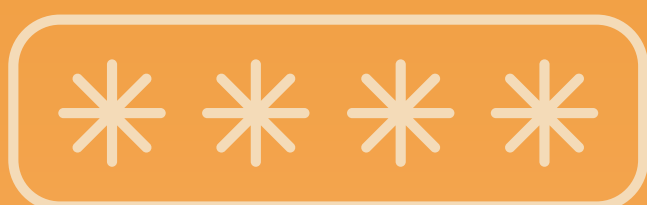
5 PRATIQUES DE CYBER RÉSILIENCE INDISPENSABLES

ACCÈS SÉCURISÉ ET AUTHENTIFICATION



Renforcez la sécurité avec l'authentification multifacteurs (MFA) et appliquez une politique "Zero Trust" de contrôle des identités et des droits d'accès.

SÉCURITÉ DES DONNÉES ET DES SYSTÈMES



Chiffrez les données sensibles, et assurez une redondance fiable et sécurisée pour une récupération rapide en cas d'incident.

PROTECTION DES TERMINAUX ET DU RÉSEAU

Sécurisez le réseau, les mails et les points de terminaison (PC, mobiles) qui constituent les principales portes d'entrée des programmes malveillants.



SURVEILLANCE ET GESTION DES INCIDENTS

Assurez la supervision et le pilotage des mesures de prévention et détection d'intrusions, et préparez un plan d'intervention en cas d'incident.

SENSIBILISATION ET AMÉLIORATION CONTINUE

Formez les employés aux bonnes pratiques de sécurité et évaluez régulièrement les processus pour les améliorer.



Vous désirez obtenir plus d'informations ?

Nos équipes sont à votre écoute :

contact@absyscyborg.com

absys • cyborg