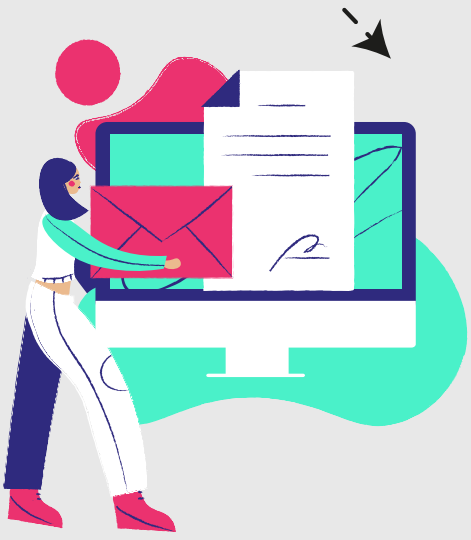
METTRE EN PLACE UNE STRATÉGIE ZERO TRUST

1 Cartographier les ressources et les accès

- Réaliser un inventaire des ressources (serveurs, applications, données...)
- Identifier les utilisateurs et leurs niveaux d'accès
- Analyser les flux de communication entre les systèmes

2 Renforcer l'authentification et l'identité

- Mettre en place une authentification multi-facteurs (MFA)
- Adopter une authentification sans mot de passe basée sur des certificats ou des clés FIDO2
- Utiliser l'authentification conditionnelle
- Implémenter une gestion stricte des comptes à privilèges via un Privileged Access Management (PAM)



3 Appliquer le principe du Least Privilege Access

- Mettre en place des politiques RBAC (Role-Based Access Control)
- Appliquer le Just-In-Time Access pour fournir des accès temporaires
- Segmenter les comptes pour éviter l'usage excessif des privilèges
- Sécuriser les identifiants et les secrets via des coffres-forts numériques

4 Surveiller en permanence les activités

- Déployer un SIEM pour centraliser les logs
- Configurer des alertes automatique
- Automatiser la réponse aux incidents
- Effectuer des audits réguliers pour identifier les failles et ajuster la politique d'accès

5 Sensibiliser les collaborateurs

La cybersécurité ne repose pas uniquement sur la technologie, mais aussi sur les bonnes pratiques des utilisateurs. Des formations régulières permettent de réduire considérablement les risques de phishing et d'attaques internes.

epsight

www.epsight.fr