Infiny Link
Informatique & Telecoms

Le Plan de Reprise d'Activité

La clé pour prévenir les attaques et assurer la continuité de votre entreprise

CHIFFRES CLES

3/4

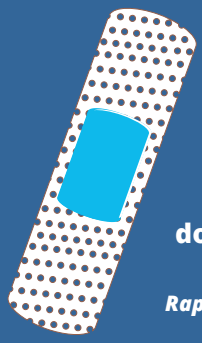
des entreprises admettent avoir été confrontées à la perte de données critiques

Etude Arcserve -2022

83%

des entreprises estiment qu'un temps d'arrêt des systèmes critiques de 12 heures est le maximum acceptable pour éviter un impact négatif mesurable sur l'entreprise

Etude Arcserve -2022



59%

des entreprises récupèrent leurs données après une cyberattaque et le paiement d'une rançon

Rapport Hiscox 2022 sur la gestion des cyber-risques

45%

des PME ne disposent pas de pare-feu

17%

des PME ont un antivirus inefficient (version gratuite, bridée ou périmée)

43%

des PME se sentent désemparés face aux offres de protection des données

AxbX Observatoire des menaces -2023

QUE SIGNIFIE UN PRA ?

Le Plan de Reprise d'Activité (PRA) est un plan détaillé qui permet aux entreprises de continuer à fonctionner en cas de perturbations majeures.

Pour les PME, cela peut inclure des événements tels qu'un incendie, une inondation, une panne de courant, une cyberattaque ou une pandémie.

Un PRA bien conçu peut aider une PME à minimiser les perturbations et les pertes financières causées par ces événements.

POURQUOI LES PME EN ONT-ELLES BESOIN ?

Les PME ont besoin d'un PRA pour assurer leur survie et leur réussite à long terme. Les incidents peuvent se produire à tout moment et les PME doivent être préparées pour y faire face.

Un PRA peut aider les PME à éviter les temps d'arrêt prolongés et les coûts élevés associés à une interruption des activités. Il peut également aider les PME à garantir la sécurité des employés et la continuité de leurs activités.

COMMENT UN PRA PEUT AIDER LES ENTREPRISES PME À MINIMISER LES PERTURBATIONS ET LES PERTES FINANCIÈRES ?

Le PRA est un élément clé de la gestion des risques pour les PME. En évaluant les risques potentiels et en planifiant une réponse adéquate, les PME peuvent minimiser les impacts négatifs des perturbations et assurer leur reprise rapide.

COMMENT ÉVALUER LES RISQUES QUI POURRAIENT PERTURBER LES ACTIVITÉS DES PME ?

L'évaluation des risques est une étape essentielle pour la mise en place d'un PRA efficace pour les PME. Elle permet de déterminer les risques qui pourraient perturber les activités des PME et de planifier une réponse adéquate à chaque risque potentiel.

L'évaluation des risques doit être menée régulièrement pour assurer la pertinence du PRA.

COMMENT PLANIFIER UNE RÉPONSE ADÉQUATE À CHAQUE RISQUE POTENTIEL POUR LES PME ?

La planification pour les PME implique la création d'un plan de communication et de sauvegarde des données en cas de perturbation majeure.

Le plan de communication doit inclure une liste de contacts clés, une méthode de communication alternative en cas de panne des systèmes habituels et des instructions claires pour la coordination et la communication des actions à prendre.

La sauvegarde des données est essentielle pour garantir la continuité des activités en cas de perte de données due à une perturbation.

COMMENT ÉLABORER UN PLAN DE COMMUNICATION ET DE SAUVEGARDE DES DONNÉES POUR LES PME ?

La planification doit également inclure des procédures d'urgence pour chaque risque potentiel.

Ces procédures doivent être clairement définies et documentées pour garantir une réponse rapide et efficace en cas de perturbation.

COMMENT METTRE EN ŒUVRE EFFICACEMENT LE PRA POUR LES PME ?

La mise en œuvre du PRA pour les PME implique la création d'un plan détaillé et l'attribution de responsabilités claires pour chaque tâche.

Il est important de veiller à ce que le PRA soit cohérent avec les objectifs commerciaux de la PME et de garantir que les ressources nécessaires sont disponibles pour mettre en œuvre le plan.

COMMENT TESTER RÉGULIÈREMENT LE PRA POUR LES PME AFIN DE GARANTIR SON EFFICACITÉ ?

Le test régulier du PRA est essentiel pour garantir son efficacité en cas de perturbation majeure.

Les tests peuvent être effectués sur une base planifiée ou inopinée et doivent impliquer l'ensemble du personnel de la PME.

Les tests peuvent inclure des simulations de perturbations, des tests de sauvegarde de données et des tests de communication.

Les résultats des tests doivent être documentés et examinés pour améliorer continuellement le PRA.

COMMENT FORMER ET SENSIBILISER LES EMPLOYÉS ?

Il est également important de former régulièrement les employés de la PME aux procédures d'urgence et de les tenir informés des modifications apportées au PRA.

Vous trouverez d'ailleurs en dernière page de ce livre blanc une liste d'actions que peuvent entreprendre en les salariés en cas d'incident ou suspicion d'attaque

La mise en place d'un PRA efficace peut aider les PME à réaliser des avantages commerciaux importants.

Cela peut inclure une meilleure résilience de l'entreprise face aux perturbations, une réduction des temps d'arrêt, une amélioration de la satisfaction des clients et des employés, une réduction des pertes financières et une amélioration de la confiance des parties prenantes.

Un PRA bien conçu favorise les PME à se conformer aux réglementations et aux normes de l'industrie. Cela peut améliorer la réputation de l'entreprise et renforcer sa position concurrentielle.

Enfin, la mise en place d'un PRA aide les PME à identifier les domaines d'amélioration et à améliorer leur efficacité opérationnelle.

En évaluant les risques et en planifiant une réponse adéquate, les PME identifient les processus inefficaces et mettent en place des améliorations pour augmenter leur productivité et leur rentabilité.

LES 7 ACTIONS A MENER D'URGENCE EN CAS D'ATTAQUE SUSPECTEE OU AVEREE

1.	**Déconnectez-vous** : Les salariés doivent déconnecter immédiatement leur ordinateur ou tout autre appareil de l'Internet en cas de suspicion de cyberattaque ou d'intrusion dans le système.
2.	**Alertez les responsables** : Les salariés doivent alerter immédiatement leur supérieur hiérarchique ou l'équipe de sécurité informatique de l'entreprise.
3.	**Changez les mots de passe** : Les salariés doivent changer immédiatement leurs mots de passe pour tous les comptes professionnels et personnels utilisant des informations similaires.
4.	**Sauvegardez les données** : Si possible, les salariés doivent sauvegarder immédiatement les données importantes sur des serveurs sécurisés et hors site pour éviter toute perte de données en cas de sinistre.
5.	**Ne pas divulguer d'informations confidentielles** : Les salariés doivent éviter de divulguer des informations confidentielles, telles que des mots de passe ou des informations de compte, par e-mail ou par téléphone.
6.	**Suivez les directives de sécurité informatique** : Les salariés doivent suivre les directives de sécurité informatique établies par leur entreprise, telles que l'utilisation de logiciels antivirus, de pare-feux et de mots de passe complexes.
7.	**Informez les collègues** : Les salariés doivent informer leurs collègues de l'incident afin qu'ils puissent prendre des mesures pour protéger leur propre système.

Infiny Link
Informatique & Telecoms

Pour en savoir plus,
www.infinylink.fr
0 811 09 41 11