



Livre blanc Altevia Tech Édition BTP

Cybersécurité
et Entreprises du BTP

Assurer la continuité des chantiers, sécuriser les données, éviter les blocages opérationnels

Préambule

Dans une entreprise du BTP, la performance repose sur la coordination entre le terrain et le bureau.

Plans, documents, plannings, devis, facturation et échanges opérationnels dépendent aujourd'hui directement du **système informatique**.

Cette dépendance est forte, mais souvent peu formalisée.
Or, la moindre indisponibilité peut bloquer un chantier, retarder une livraison ou désorganiser une équipe.

La cybersécurité n'est plus un sujet technique réservé au bureau.
Elle est devenue une condition directe de la **continuité opérationnelle** et du **respect des délais**.

Ce livre blanc s'adresse aux dirigeants d'entreprises du BTP qui souhaitent

- comprendre les risques réels
- structurer une approche claire
- assumer un cadre durable et maîtrisé
- sans céder à la complexité ni à la peur.

L'informatique comme levier de continuité chantier

Une entreprise du BTP moderne dépend de son informatique pour

- l'accès aux plans et documents techniques
- la communication entre terrain et bureau
- la gestion des plannings
- la facturation et le suivi administratif
- la coordination avec les sous traitants

Les équipes travaillent de plus en plus en mobilité, avec des outils simples mais indispensables.

La moindre indisponibilité peut avoir un impact immédiat sur

- un blocage opérationnel
- des retards de chantier
- une perte de productivité immédiate
- des tensions avec les clients et partenaires

**Dans ce contexte, l'informatique n'est plus un support.
C'est un levier clé de continuité chantier.**

La nature spécifique des risques cyber pour le BTP

Des environnements hétérogènes et exposés

Les entreprises du BTP utilisent des données financières sensibles

- des postes fixes et mobiles
- des smartphones et tablettes terrain
- des accès partagés
- des outils parfois peu sécurisés

Cette hétérogénéité augmente fortement la surface de risque.

Une exposition opérationnelle directe

Un incident informatique peut provoquer

- l'impossibilité d'accéder aux plans
- la perte de documents contractuels
- l'arrêt de la coordination terrain bureau
- des retards aux conséquences financières

**Dans le BTP, un incident cyber est rarement abstrait.
Il se traduit par un chantier bloqué.**

Les fausses certitudes les plus répandues

Ce que beaucoup de d'entreprises du BTP pensent

De nombreux dirigeants pensent être protégés car

- leurs outils sont simples
- elles n'ont pas beaucoup de données
- elles n'ont jamais eu d'incident
- leurs équipes savent se débrouiller

Ces éléments sont nécessaires mais très insuffisants.

Ce que montrent les incidents réels

La majorité des incidents graves surviennent dans des environnements

- peu structurés
- mal sécurisés
- avec des accès partagés
- sans responsabilité clairement définie

**La cybersécurité ne se résume pas à des outils.
Elle repose avant tout sur une organisation claire et adaptée
au terrain.**

Le changement de paradigme nécessaire

La cybersécurité efficace repose sur trois principes fondamentaux.

La simplicité

- Un système simple, documenté et compris est plus sécurisé qu'un système complexe et mal maîtrisé.

L'intégration

- La sécurité doit être intégrée aux usages quotidiens, sans ralentir l'activité.

La responsabilité: quelqu'un doit assumer clairement

- le bon fonctionnement
- la sécurité
- la continuité
- la réaction en cas d'incident

La cybersécurité est un cadre opérationnel à poser, pas une contrainte à subir.

Questions clés pour les dirigeants d'entreprises du BTP

Pouvez vous répondre clairement à ces questions

- vos équipes terrain peuvent elles accéder aux documents à tout moment ?
- les accès aux outils sont ils maîtrisés ?
- les appareils mobiles sont ils sécurisés ?
- les sauvegardes sont elles réellement exploitables ?
- savez vous qui intervient en cas d'incident ?
- la continuité de chantier est elle garantie ?
- vous sentez vous serein sur ce sujet ?

Si ces réponses ne sont pas immédiates, le risque existe déjà.

L'approche Altevia Tech pour les entreprises du BTP

Altevia Tech accompagne les entreprises du BTP avec une approche pensée pour la réalité du terrain

- claire
- progressive
- sans jargon inutile
- orientée continuité et efficacité opérationnelle

Nous prenons en charge l'ensemble du système informatique

- la gestion du parc informatique
- le support utilisateurs
- la supervision continue
- les sauvegardes et la continuité d'activité
- la gestion des accès et des identités

La cybersécurité est intégrée par défaut.

Elle s'adapte aux usages terrain sans les freiner.

Objectif

- un système fiable
- des équipes opérationnelles
- une continuité garantie
- un dirigeant serein

Nous assumons la responsabilité du bon fonctionnement de votre informatique.

Une méthode progressive et adaptée au terrain

Notre démarche repose sur une progression maîtrisée

- identifier les risques concrets
- stabiliser le socle
- définir une trajectoire pragmatique
- superviser et améliorer dans le temps

Vous démarrez simplement.

Nous sécurisons sans perturber vos chantiers.

Conclusion

La cybersécurité dans le BTP n'est pas une contrainte supplémentaire.

C'est une condition de continuité opérationnelle.

Une entreprise du BTP qui maîtrise son informatique

- évite les blocages
- sécurise ses chantiers
- protège ses données
- travaille plus efficacement.

Avec Altevia Tech, vous faites le choix

- d'un partenaire responsable
- d'un cadre clair
- d'une sécurité intégrée
- d'une informatique qui ne soit plus jamais un sujet.



Prochaines étapes

Un diagnostic cybersécurité confidentiel pour les entreprises du BTP

- une analyse factuelle
- des priorités claires
- une vision maîtrisée

Pour en discuter

contact@altevia-tech.com
www.altevia-tech.com

