

Votre score : 10 / 20

Ça tient... tant que rien ne bouge

Votre informatique fonctionne, mais elle repose sur quelques angles morts.

Votre informatique fait le travail au quotidien. Le risque n'est pas aujourd'hui, c'est le jour où quelque chose change : un départ, une panne, un client qui pose une question précise. Voici les deux ou trois endroits où ça peut coïncider, avec ce que ça coûterait.

Comment lire ce rapport

1. La synthèse (page 2) : vos angles morts et ce qu'ils coûtent.
2. Dix chapitres, un par question : ce que votre réponse veut dire, trois actions concrètes avec le temps qu'elles prennent, et ce que Sérénitique prend en charge si vous préférez déléguer.
3. Un plan sur 30 jours et la liste des documents qu'un client ou un assureur vous demandera.

Ce rapport est généré à partir de vos réponses. Il ne remplace pas un audit, mais il vous dit par où commencer, avec ou sans prestataire.

Synthèse

Vos angles morts, et leur impact

Le savoir est dans des têtes, pas dans des outils

Des fichiers ou des mots de passe qui ne vivent que sur un PC ou dans une tête, c'est un arrêt d'activité en attente. Centraliser documents et accès (espace partagé, gestionnaire de mots de passe) se règle en quelques jours.

Les pannes sont découvertes par vos équipes

Si c'est vous qui détectez les pannes, personne ne surveille votre informatique. Une supervision continue voit un disque qui fatigue ou une sauvegarde qui échoue avant que l'équipe ne soit bloquée.

Le coût d'une panne n'est pas chiffré

Une matinée sans serveur ni messagerie, c'est quatre heures de chiffre d'affaires perdues, plus le retard accumulé. Chiffrer ce coût est la première étape pour décider combien investir dans sa prévention.

Combien coûte une matinée sans informatique ?

Repère : une PME réalisant 2 M€ par an sur 220 jours de 8 heures génère environ 1 140 € par heure. Une matinée sans serveur ni messagerie (4 heures) représente 4 500 € de chiffre d'affaires, avant le retard accumulé. Faites le calcul avec vos chiffres : $CA \text{ annuel} \div 1\,760 \text{ heures} \times 4$.

Vos réponses

- 1. Le coût réel d'une panne : À peu près
- 2. Continuité quand quelqu'un s'absente : Non, on attend son retour
- 3. Arrivées et départs : Oui, tout est prêt
- 4. Prévisibilité du budget : Sauf quelques surprises
- 5. Preuves de sécurité pour vos clients et assureurs : Je dirais « on fait attention »
- 6. Le temps volé au métier : Oui, de temps en temps
- 7. Supervision et détection : Nous, et on a attendu
- 8. Sauvegardes et reprise d'activité : « On a des sauvegardes, je crois »
- 9. Une informatique au niveau de l'entreprise : Oui, et l'informatique a suivi
- 10. Un partenaire qui prévient : Ça arrive, rarement

1

Le coût réel d'une panne

Votre réponse : À peu près

Vous avez un ordre de grandeur. Précisez-le : c'est lui qui dit combien il est raisonnable d'investir dans la prévention.

Trois actions concrètes

1. Calculez votre CA par heure

10 min

CA annuel ÷ 220 jours ÷ 8 heures. Multipliez par 4 : c'est le prix d'une matinée sans informatique, avant le retard accumulé et les clients qui attendent.

2. Listez vos trois outils critiques

15 min

Messagerie, logiciel métier, serveur de fichiers : lesquels arrêtent vraiment l'activité quand ils tombent ? Ce sont eux à protéger en premier.

3. Fixez un budget prévention

30 min

Un forfait mensuel d'infogérance coûte en général moins qu'une seule matinée d'arrêt par an. Mettez les deux chiffres côte à côte.

Avec Sérénitique : Le forfait mensuel fixe couvre supervision, maintenance et support : vous connaissez le coût de la prévention avant de signer.

2

Continuité quand quelqu'un s'absente

Votre réponse : Non, on attend son retour

Une partie de votre entreprise s'arrête avec chaque absence. C'est un risque de continuité, pas un détail d'organisation.

Trois actions concrètes

1. Inventaire des accès critiques

1 h

Pour chaque logiciel et chaque compte : qui a l'accès, où est le mot de passe, qui peut le récupérer en cas d'absence.

2. Gestionnaire de mots de passe partagé

Une matinée

Bitwarden, 1Password ou Keeper : un coffre par équipe, un accès de secours pour la direction, plus aucun mot de passe sur un post-it ou dans une tête.

3. Espace documentaire commun

Une semaine

Les dossiers de travail sur un espace partagé (serveur, SharePoint, Drive). Plus rien d'important sur un seul ordinateur.

Avec Sérénitique : Gestion des accès et des comptes incluse, arrivées et départs traités le jour même, documentation du parc tenue à jour pour vous.

Arrivées et départs

Votre réponse : Oui, tout est prêt

Les arrivées sont industrialisées : poste, comptes et accès prêts le jour J. Vos recrues le remarquent.

Trois actions concrètes

1. Check-list d'arrivée

30 min

Poste, messagerie, logiciels, badge, mot de passe initial : une liste, un responsable, tout prêt à J-2.

2. Poste type prêt à l'emploi

Une demi-journée

Une image de poste standard avec vos logiciels et réglages : la préparation passe de quatre heures à trente minutes.

3. Procédure de départ

30 min

Le jour du départ : accès coupés, messagerie redirigée, matériel récupéré, mots de passe partagés changés. Sans exception.

Avec Sérénitique : Onboarding et offboarding inclus dans le forfait : poste préparé avant l'arrivée, accès coupés le jour du départ.

Prévisibilité du budget

Votre réponse : Sauf quelques surprises

Les « quelques surprises » sont souvent les lignes les plus chères de l'année : un serveur qui lâche, un dépannage de nuit.

Trois actions concrètes

1. Relevez les dépenses IT des 12 derniers mois

1 h

Matériel, licences, dépannages, abonnements, temps interne : le total surprend presque toujours.

2. Séparez récurrent et imprévu

30 min

Ce qui est imprévu est précisément ce qu'un contrat de maintenance doit absorber. Le reste se budgete.

3. Planifiez les renouvellements

1 h

Âge de chaque serveur et de chaque poste : au-delà de cinq ans, prévoyez le remplacement avant la panne, pas après.

Avec Sérénitique : Un forfait mensuel fixe, tout inclus, fixé à la signature. Pas de dépannage à l'heure, pas de déplacement facturé en plus.

Preuves de sécurité pour vos clients et assureurs

Votre réponse : Je dirais « on fait attention »

« On fait attention » ne rassure ni un client, ni un assureur, ni un auditeur. Il faut l'écrire.

Trois actions concrètes

1. Rédigez la page « Comment nous protégeons vos données » 2 h

Sauvegardes, accès, mises à jour, antivirus, plan de reprise, qui contacter. Une page suffit, et elle se réutilise à chaque appel d'offres.

2. Relisez votre contrat d'assurance cyber 30 min

Quelles mesures sont exigées ? Sauvegardes testées, double authentification, mises à jour : cochez ce qui manque, c'est votre liste de priorités.

3. Désignez un responsable 10 min

Une personne qui répond aux questions sécurité et tient la page à jour, même si c'est votre prestataire.

Avec Sérénitique : Audit de sécurité, documentation de vos mesures, accompagnement sur l'assurabilité et NIS2. Sérénitique est membre de la Fédération Française de la Cybersécurité.

Le temps volé au métier

Votre réponse : Oui, de temps en temps

Un collaborateur bricole « de temps en temps » : comptez les heures, elles ne sont jamais facturées mais toujours payées.

Trois actions concrètes

1. Mesurez le temps réel 2 semaines

Notez chaque intervention informatique faite en interne : qui, combien de temps, pour quoi. Deux semaines suffisent pour voir la tendance.

2. Valorisez-le 10 min

Heures × coût horaire chargé. Comparez ce montant au coût d'un forfait d'infogérance.

3. Décidez ce qui reste en interne 30 min

Le premier niveau (redémarrer, rebrancher) peut rester. La sécurité, les sauvegardes et les serveurs, non.

Avec Sérénitique : Support illimité de vos équipes, un numéro unique, 95 % des incidents réglés à distance : vous ne gérez plus rien.

Supervision et détection

Votre réponse : *Nous, et on a attendu*

Personne ne surveille votre informatique. Chaque panne est découverte par un collaborateur bloqué, au pire moment.

Trois actions concrètes

1. Listez les cinq équipements vitaux

15 min

Serveur, box internet, NAS, pare-feu, messagerie : ce qui doit être surveillé en priorité.

2. Activez les alertes de base

1 h

Espace disque, sauvegarde en échec, mises à jour en attente : la plupart des outils savent envoyer un e-mail. Encore faut-il qu'il arrive à quelqu'un.

3. Exigez un rapport mensuel

10 min

Demandez à votre prestataire un point écrit chaque mois : incidents, mises à jour, sauvegardes vérifiées. S'il ne peut pas, c'est une réponse.

Avec Sérénitique : Supervision 24h/24 des postes et serveurs, alertes traitées avant que l'équipe ne soit bloquée, point mensuel sans jargon.

Sauvegardes et reprise d'activité

Votre réponse : « On a des sauvegardes, je crois »

« On a des sauvegardes, je crois » est la phrase la plus dangereuse de ce questionnaire. Une sauvegarde non testée n'existe pas.

Trois actions concrètes

1. Test de restauration

20 min, dès lundi

Restaurez un fichier d'hier. Puis un dossier complet. Notez la date et le résultat. Recommencez chaque trimestre.

2. Règle 3-2-1

Une demi-journée

Trois copies, sur deux supports, dont une hors site ou déconnectée. Une sauvegarde accessible en réseau est chiffrée avec le reste lors d'une attaque.

3. Plan de reprise écrit

2 h

Qui appeler, dans quel ordre, combien de temps pour redémarrer, où sont les sauvegardes. Une page, imprimée, hors de l'ordinateur.

Avec Sérénitique : Sauvegardes automatiques testées, plan de reprise d'activité écrit et exercé, isolation d'urgence des comptes et serveurs compromis.

Une informatique au niveau de l'entreprise

Votre réponse : Oui, et l'informatique a suivi

Votre informatique a suivi la croissance : bon signe. Continuez à la revoir à chaque changement important.

Trois actions concrètes

1. État des lieux du parc

2 h

Liste des postes, serveurs, comptes et abonnements, avec leur âge. Ce qu'on ne liste pas, on ne protège pas.

2. Sécurisez le télétravail

Une demi-journée

VPN ou accès cloud avec double authentification, ordinateurs chiffrés, plus de documents sensibles qui circulent par e-mail.

3. Nettoyez les comptes

1 h

Supprimez les comptes des anciens salariés, réduisez les droits administrateur à ceux qui en ont vraiment besoin.

Avec Sérénitique : Reprise du parc existant sans interruption, remise à niveau, puis maintenance proactive pour que l'installation suive l'entreprise.

Un partenaire qui prévient

Votre réponse : Ça arrive, rarement

Ça arrive, rarement : votre partenaire est surtout en mode réparation. Posez-lui la question de la supervision.

Trois actions concrètes

1. Demandez un bilan annuel

10 min

À votre prestataire, ou à vous-même : qu'est-ce qui a cassé cette année, et qu'est-ce qui aurait pu être évité ?

2. Planifiez les mises à jour

30 min

Un créneau hebdomadaire hors heures de travail pour les mises à jour de sécurité des postes et serveurs.

3. Comparez les modèles

1 h

Un contrat au forfait, prévention incluse, contre votre coût actuel : dépannages, temps interne et pannes additionnés.

Avec Sérénitique : Maintenance proactive, mises à jour planifiées de nuit, disques remplacés avant de lâcher : un partenaire qui appelle pour éviter la panne.

Votre plan sur 30 jours

Huit actions, deux par semaine, chacune faisable en interne. Celles marquées « priorité » répondent directement à vos réponses les moins solides.

- | | | | |
|--------------------------|-----------|--|--------------------|
| ☐ | SEMAINE 1 | Tester une restauration de sauvegarde et noter le résultat | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 1 | Inventorier les accès critiques : qui, où, comment les récupérer | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 2 | Mettre en place un gestionnaire de mots de passe partagé | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 2 | Activer la double authentification sur la messagerie, direction d'abord | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 3 | Rédiger la page « Comment nous protégeons vos données » | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 3 | Écrire la check-list d'arrivée et la procédure de départ | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 4 | Faire l'état des lieux du parc, avec l'âge de chaque équipement | PRIORITÉ POUR VOUS |
| ☐ | SEMAINE 4 | Comparer le coût actuel (pannes, temps interne, dépannages) à un forfait | |

Au bout de 30 jours

Vous saurez si vos sauvegardes fonctionnent, où sont vos accès, ce que coûte votre informatique et ce qu'elle devrait coûter. C'est exactement le point de départ d'une discussion utile, avec nous ou avec un autre partenaire.

Le dossier que vos clients et assureurs vous demanderont

Dix documents. Aucun n'est compliqué à produire, tous font la différence le jour où un donneur d'ordre, un assureur cyber ou un auditeur pose la question. Cochez ce que vous avez déjà.

- ☐ Inventaire du parc (postes, serveurs, comptes, abonnements) daté de moins d'un an
- ☐ Politique de mots de passe et gestionnaire en place
- ☐ Preuve de la dernière restauration de sauvegarde testée, avec sa date
- ☐ Plan de reprise d'activité écrit, avec les contacts d'urgence
- ☐ Liste des accès et des droits administrateur, revue à chaque départ
- ☐ Procédure d'arrivée et de départ des collaborateurs
- ☐ Journal des mises à jour de sécurité des postes et serveurs
- ☐ Contrat de maintenance ou d'infogérance avec le périmètre couvert
- ☐ Page « Comment nous protégeons vos données » à remettre à un client ou un assureur
- ☐ Attestation ou rapport du dernier audit de sécurité

Pourquoi maintenant

La directive NIS2 étend les obligations de cybersécurité à de nombreuses PME de la chaîne de sous-traitance, et les assureurs conditionnent désormais leurs garanties à des mesures vérifiables. Un dossier prêt vaut un marché gardé.

Pour aller plus loin avec Sérénitique

Sérénitique accompagne les PME et TPE de Bourgogne depuis 2008, depuis Beaune, avec 25 collaborateurs. Membre de la Fédération Française de la Cybersécurité. Tout ce que décrit ce rapport, nous pouvons le prendre en charge, dans un forfait mensuel fixe.

Infogérance au forfait

Supervision, maintenance, support illimité de vos équipes, sauvegardes testées : un montant mensuel fixé à la signature, sans dépannage à l'heure ni déplacement facturé.

Surveillance de la sécurité 24h/24

Vos comptes et serveurs sous surveillance continue, isolation d'urgence en cas de compromission, selon votre forfait.

Plan de reprise d'activité

Un plan écrit, des sauvegardes hors site, un test de restauration planifié : la preuve que vous pouvez redémarrer.

Audit de sécurité et pentest

Pour les entreprises qui doivent répondre à un client, un assureur ou NIS2 avec des preuves.

Formations

Office 365 et cybersécurité pour vos équipes : moins d'erreurs humaines, plus d'autonomie.

Si vous voulez qu'on regarde vos réponses ensemble : 20 minutes, sans engagement et sans PowerPoint.

calendly.com/david-serenitique/20min · 03 80 20 16 74 · service@serenitique.fr

Sérénitique · 3 impasse Jean-Baptiste Gambut, 21200 Beaune · serenitique.fr