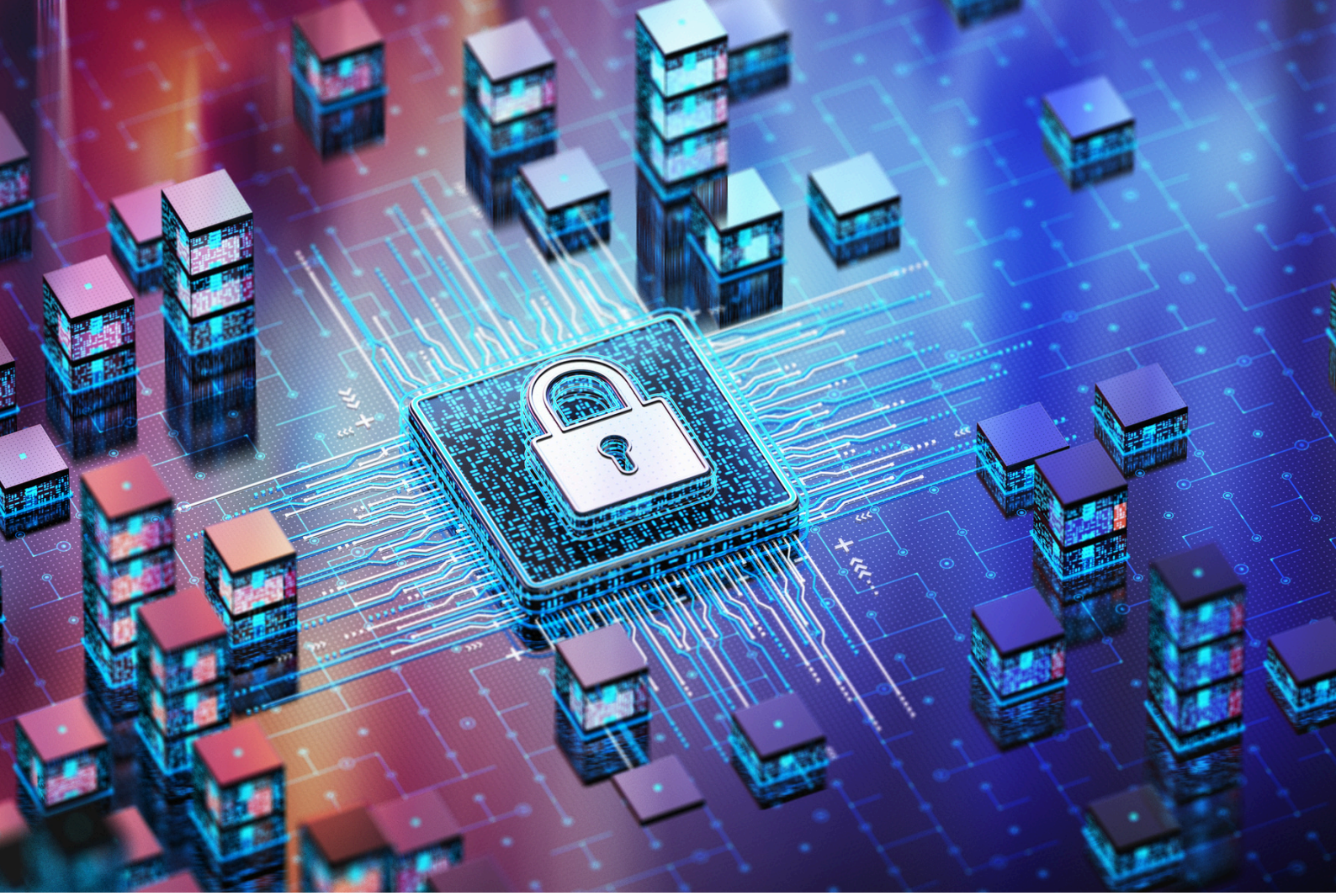


CYBERSÉCURITÉ D'ENTREPRISE : GUIDE PME

Comment bâtir une protection sur-mesure avec accompagnement expert ?

CELESTE

La cybersécurité n'est plus une affaire réservée aux grandes entreprises. Aujourd'hui, 60% des cyberattaques en France ciblent les petites et moyennes entreprises (PME). Pourquoi ? Parce qu'elles sont perçues comme plus vulnérables, souvent mal équipées, et insuffisamment accompagnées.

Ce guide vise à clarifier les risques réels liés à la sécurité informatique, et surtout, à identifier les leviers concrets pour mieux protéger son système d'information. Tout au long du parcours, Gautier Aldebert, Ingénieur Avant Vente chez CELESTE, apporte ses conseils issus du terrain, ses retours d'expérience, et des recommandations directement applicables.

Sommaire

1 Cyberattaques PME : mieux détecter, mieux anticiper

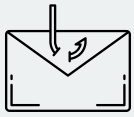
Rançongiciels, phishing, DDoS, usurpation d'identité... Les PME sont des cibles de choix pour les cybercriminels, en raison de failles techniques et organisationnelles fréquentes : absence de politique de sécurité, configurations faibles, manque de formation. Comprendre ces risques, c'est déjà renforcer sa posture de sécurité.

«Aujourd'hui, croire qu'un simple pare-feu suffit est illusoire. Les cyberattaques ne visent plus seulement les failles techniques, mais aussi les vulnérabilités humaines, organisationnelles et applicatives.
Mal configuré ou non mis à jour, un pare-feu peut même devenir une porte d'entrée. C'est l'ensemble de l'environnement numérique qu'il faut structurer et sécuriser.

Les cybermenaces les plus fréquentes pour les PME

Rançongiciel

Blocage des systèmes, demande de rançon



Phishing

Vol d'identifiants via e-mails piégés

Attaques DDoS

Saturation des serveurs

Usurpation d'identité

Faux e-mails ou ordres de virement

Malware

Logiciels malveillants infiltrant le réseau

1 Les Cyberattaques PME : mieux détecter, mieux anticiper

Les angles morts qui fragilisent votre sécurité IT

Trop souvent, les cyberattaques réussissent non pas par la complexité des méthodes employées, mais à cause des **failles internes** connues mais négligées. De nombreuses PME sous-estiment certains aspects essentiels de leur sécurité, laissant la porte ouverte à des menaces évitables.

Les 4 faiblesses critiques des PME en matière de cybersécurité

La plupart des cyberattaques ciblant les PME reposent moins sur des techniques complexes que sur des failles de base. Voici les erreurs les plus courantes observées sur le terrain :

Absence de politique de sécurité informatique
Sans cadre défini, les collaborateurs naviguent à vue, multipliant les comportements à risque.

Manque de formation des équipes
Un simple clic mal placé peut ouvrir une brèche. Or, la sensibilisation reste souvent absente.

Équipements obsolètes ou mal configurés
Un routeur ou un pare-feu mal paramétré devient une porte d'entrée directe pour un attaquant.

Pas d'analyse proactive des risques
Trop souvent, la cybersécurité est réactive : on agit après l'incident, rarement avant.*

Une faille humaine ou technique suffit à compromettre tout un système !

2 Analyse métier : première étape vers une sécurité efficace

La cybersécurité commence par une bonne compréhension du métier

Avant de déployer des outils ou d'investir dans une solution de cybersécurité, il est essentiel de comprendre d'abord les spécificités métier de chaque PME. Une agence digitale, un cabinet d'expertise comptable ou encore un distributeur e-commerce n'ont ni les mêmes risques, ni les mêmes priorités opérationnelles. Pourtant, nombre d'entreprises abordent encore la cybersécurité comme un sujet purement technique.

Chez CELESTE, nous constatons chaque jour que les menaces les plus critiques varient selon l'activité, le type de données manipulées et surtout les usages numériques. C'est pourquoi un diagnostic initial personnalisé est indispensable: il permet d'identifier les véritables points de vulnérabilité et d'y répondre de manière ciblée.

Ce qu'une analyse métier permet de révéler	
Les actifs critiques Données, outils et services essentiels au bon fonctionnement	**Les usages à risque** Comportements métiers ou outils non encadrés
Les failles invisibles Configurations négligées, accès trop larges, absence de contrôle	**Les priotités réelles** Ce qu'il faut protéger en premier selon vos enjeux métier

2 Analyse métier : première étape vers une sécurité efficace

Une stratégie de cybersécurité alignée avec vos priorités

Ce diagnostic métier permet ensuite de construire une stratégie sur-mesure, à la fois technique, humaine et organisationnelle. C'est la seule voie pour une cybersécurité pérenne et réellement efficace.

En travaillant main dans la main avec ses clients PME, CELESTE apporte un regard extérieur expert et une méthode structurée, pensée pour protéger l'essentiel : vos données, vos services, votre réputation.

On pensait être bien protégés...

Beaucoup de dirigeants découvrent, lors de cet exercice, que leur couverture n'est que partielle. L'analyse métier agit comme un révélateur, sans jargon, mais avec des indicateurs concrets qui permettent de décider et d'agir.

Tout démarre par une analyse fine du métier et des usages : il ne s'agit pas de déployer des outils pour cocher des cases, mais bien de cibler les vrais points de vulnérabilité.

Chez CELESTE, notre approche part toujours d'un diagnostic précis : comprendre le fonctionnement de l'entreprise, ses priorités, son exposition. C'est la seule manière de construire une stratégie cohérente. La cybersécurité consiste à sécuriser ce qui compte vraiment, là où les risques sont les plus critiques.

3 Protéger et superviser : une cybersécurité durable pour votre PME

Protégez votre système d'information

La cybersécurité ne s'improvise pas : elle repose sur des **technologies adaptées, déployées avec rigueur et cohérence.** Chez CELESTE, nous sélectionnons des solutions alignées sur votre activité, vos contraintes métiers et vos priorités de sécurité.

Chaque outil est configuré, supervisé et maintenu par nos équipes pour assurer une protection continue et fiable. Notre objectif : **créer un environnement numérique sécurisé, évolutif et sans surcharge** inutile pour vos équipes.

Solutions clés de CELESTE

Pare-feu managé avec filtrage web intelligent
Solutions UTM pour une défense tout-en-un
Filtrage e-mail avancé (anti-spam, antivirus)
VPN sécurisé pour les accès distants
Protection Anti-DDoS pour les sites exposés
Wi-Fi pro sécurisé avec portail captif

👉 Découvrez notre approche modulaire ici

Chez CELESTE, nous concevons une cybersécurité opérationnelle, pensée pour s'intégrer à votre environnement métier, quel que soit votre secteur d'activité. L'objectif ? Déployer les bons outils, au bon endroit, et garantir leur efficacité dans le temps grâce à une supervision proactive

3 Protéger et superviser : une cybersécurité durable pour votre PME

Superviser pour rester protéger

La cybersécurité ne se limite pas à l'installation d'outils performants. Elle repose sur leur supervision continue, leur configuration adaptée et leur mise à jour régulière. Sans ces actions de suivi — ce qu'on appelle le **Maintien en Condition Opérationnelle (MCO)** — même un pare-feu peut devenir une faille exploitable.

Qu'est-ce que le MCO (Maintien en Condition Opérationnelle) ?

Le MCO est l'ensemble des actions et processus visant à garantir que les systèmes et équipements restent fonctionnels et performants. Cela inclut la maintenance préventive, les réparations, les mises à jour et la surveillance continue pour assurer la disponibilité et la fiabilité des services essentiels.

Le saviez vous ?

La plupart des failles ne viennent pas d'un manque de technologie, mais d'un manque d'accompagnement dans son déploiement et son usage.

Ce n'est pas au moment de l'attaque qu'il faut découvrir une faille. La supervision continue est ce qui fait toute la différence. Elle assure que vos systèmes restent performants face à des menaces en constante évolution

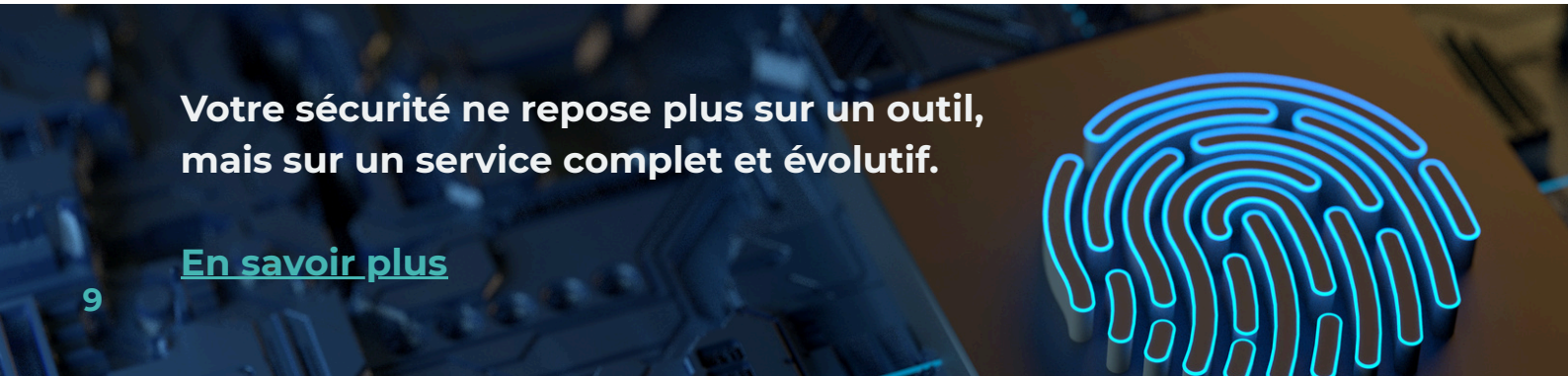
4 Tests d’intrusion et ajustements

Mettre en place des protections, c’est indispensable. Mais sans les tester, leur efficacité reste théorique. Les tests d’intrusion permettent de simuler des attaques réelles pour identifier les failles encore présentes dans le système. C’est une démarche proactive qui transforme la cybersécurité en un processus vivant et améliorable — pour renforcer les défenses avant qu’un incident ne survienne.

Pourquoi réaliser des tests d’intrusion ?

- Identifier des failles invisibles
- Améliorer la réponse en cas d’incident
- Prioriser les futures améliorations

Tester son système, c’est obtenir une vision claire de son niveau de sécurité. Cela permet de corriger les failles avant qu’elles ne soient exploitées. Trop de PME ne s’en rendent compte qu’après une attaque.



Votre sécurité ne repose plus sur un outil, mais sur un service complet et évolutif.

En savoir plus

5 *Un cap, une méthode, un Partenaire !*

La sécurité informatique ne s'improvise pas. Pour les PME, la clé réside dans une approche pragmatique, adaptée à leur réalité, et surtout accompagnée par des experts. Chez CELESTE, nous les aidons à construire des systèmes de défense cyber **cohérents, évolutifs et durables**.

L'accompagnement CELESTE en 3 étapes

Diagnostic

Déploiement

Supervision

Une question ?

Prenez rendez-vous avec un expert cybersécurité PME

Contactez-nous

info@celeste.fr

www.celeste.fr