Diagnostic Cybersécurité PME

Savoir où vous en êtes. Savoir quoi faire.

Jean Pineau — Consultant GRC Cybersécurité

jeanpineau@cybergrc.fr

01 – CONTEXTE

La cybermenace est une réalité pour les PME

Les cyberattaques ne ciblent plus seulement les grandes entreprises. Aujourd'hui, 1 entreprise sur 2 attaquée est une PME – souvent moins protégée, donc plus facile à atteindre

Les attaquants ne cherchent pas forcément à détruire :
ils cherchent à voler des données, paralyser l'activité, ou extorquer une rançon.

Pour une PME sans équipe dédiée, les conséquences peuvent être fatales.

La cybermenace en chiffres

50 %

Des PME attaquées chaque année ↗

60 k €

Coût moyen d'une cyberattaque pour une PME ↗

26 j

Durée moyenne d'interruption d'activité ↗

+50 %

de risque de défaillance dans les 6 mois suivant un incident ↗

Les conséquences

Une cyberattaque peut mettre fin à votre activité

Données volées, systèmes paralysés, messagerie compromise; les scénarios sont variés, les conséquences souvent identiques : l'activité s'arrête. Chaque jour d'arrêt représente du chiffre d'affaires perdu, des clients qui se tournent vers un concurrent et des salaires à verser sans recette.

Une entreprise touchée sur deux présente un risque de défaillance dans les six mois suivant l'incident. Pas forcément à cause de l'attaque elle-même, mais à cause du coût de la remise en route, des pénalités contractuelles et de la perte de confiance des clients. Sans compter la perte de données : fichiers client, processus en place, des années de travail à reconstruire de zéro.
Ce n'est pas qu'un problème informatique. C'est un risque de survie.

26 j

sans activité en moyenne

après une attaque réussie

Les gains potentiels

Continuité opérationnelle garantie
Anticiper, c'est ne plus subir. En réduisant drastiquement la probabilité d'une intrusion et en se préparant si cela devait arriver, vous protégez vos marges opérationnelles. Une entreprise préparée est une entreprise qui n’est pas prise par surprise et qui réduit les conséquences d’une attaque.

Protection du patrimoine et de l'image
Vos fichiers clients et vos savoir-faire sont le cœur de votre valeur. Garantir leur sécurité, c'est protéger des années de travail. Vous évitez l'impact réputationnel dévastateur d'une fuite de données et assurez la pérennité de votre marque sur le long terme.

Un levier de confiance
La cybersécurité n'est plus une option technique, c'est un prérequis commercial. En sécurisant vos actifs, vous rassurez vos partenaires financiers, répondez aux exigences légales et transformez votre conformité en un avantage concurrentiel distinctif.

48 h

La durée pour la reprise d’activité que votre entreprise doit viser

Ce que la loi vous impose

RGPD (2018)
Obligation de protéger les données personnelles de vos clients et collaborateurs. En cas de violation, amendes jusqu'à 4% du CA mondial.

NIS2
Extension des obligations de cybersécurité à de nouveaux secteurs. Les PME sous-traitantes d'entités régulées sont concernées.

Responsabilité du dirigeant
En cas de manquement avéré, la responsabilité personnelle du dirigeant peut être engagée.

4 %

du Chiffre d'affaires mondial

d'amende RGPD

Pourquoi les PME sont particulièrement exposées

Pas de Responsable de la Sécurité des Systèmes d'Information (RSSI)

La sécurité est souvent gérée par le **responsable IT ou le dirigeant** lui-même, sans formation spécialisée ni **temps dédié.**

Possèdent des données sensibles

Données clients, données financières, accès fournisseurs : les PME détiennent **des actifs à forte valeur**, souvent sans protection proportionnée.

Présence d'outils non sécurisés

Messagerie, cloud, accès distants : des usages du quotidien souvent déployés **sans configuration de sécurité** adaptée.

02 – Les offres

Trois offres, une progression claire

Offre A – Etude de périmètre – Analyse des enjeux : ce que vous devez protéger, pourquoi et qui agit dessus actuellement.

Offre B – Audit de sécurité – Audit & Plan d'action : comment le périmètre est protégé aujourd'hui. Comment amélioré la sécurité.

Offre C – Accompagnement de mise en place – Suivi d'implémentation : accompagnement à la mise en œuvre des actions identifiées.

A – Etude de périmètre – *Cartographie des enjeux*

1	**Valeurs métier* + Biens supports****	Identification des actifs critiques et des composants techniques qui les sous-tendent.
2	**Parties prenantes**	Recensement des accès informatique : collaborateurs, prestataires, connexions externes.
3	**Normes applicables**	Identification des obligations légales et contractuelles qui s'appliquent à votre activité : RGPD, NIS2, normes sectorielles.
4	**Restitution**	Rapport priorisé : actifs à protéger, justifications et niveau d'urgence.

Valeurs métier* : ce qui compte vraiment : vos **données et vos **processus**. Leur perte ou leur vol a un impact direct sur votre activité (ex. : fichier clients, facturation, gestion des stocks).*
***Biens supports* : le contenant, pas le contenu. C'est l'outil qui porte une valeur métier (ex. : un ordinateur, un logiciel, un serveur). Sa perte seule est secondaire: perdre un ordinateur, tant que les données sont sauvegardées ailleurs et inaccessibles à un attaquant présente des conséquences moindres*

A – Etude de périmètre – *Processus*

Cadrage initial

Semaine 1

Échange d'une heure avec la direction pour cadrer l'entreprise au sens large : activité, organisation, données manipulées, outils numériques, obligations réglementaires. L'objectif est d'orienter les futures étapes et d'identifier les interlocuteurs clés à mobiliser.

1h

Collecte

Semaine 1

Entretient d'une demi-journée avec vos équipes. Nous identifions vos valeurs métier, les biens supports associés, les parties prenantes et le socle de sécurité existant. Nous recensons les normes applicables et les événements redoutés pour votre activité.

½ journée

Analyse

Semaine 2

Compilation et analyse des informations recueillies. Échanges supplémentaires par e-mail si nécessaire. Rédaction d'un rapport détaillé présentant votre besoin en sécurité : données à protéger, normes applicables, état des lieux.

Restitution

Semaine 2

Réunion d'une heure pour vous présenter le besoin en sécurité identifié, parcourir les recommandations et répondre à vos questions. Nous définissons ensemble les prochaines étapes à envisager pour renforcer votre posture de sécurité.

1h ou plus

B – Audit de sécurité – *Audit & Plan d'action*

1	**Audit de sécurité**	Évaluation de 42 règles ANSSI, ciblée sur les enjeux spécifiques identifiés lors de la phase précédente.
2	**Analyse des écarts**	Analyse des écarts constatés, mis en perspective avec vos enjeux métier dans un langage accessible.
3	**Plan d'action & estimation du cout**	Actions classées selon trois axes : gain en sécurité, complexité de mise en œuvre et cout de mise en œuvre, pour distinguer les mesures immédiates des chantiers de fond.
4	**Restitution**	Rapport détaillé, présentation des résultats et session d'échange de 2h ou plus si nécessaire.

B – Audit de sécurité – *Processus*

Cadrage

Semaine 1

Suite à la partie A, votre contexte est connu.

Confirmer des interlocuteurs à solliciter pour l'audit (direction, informatique, métier…) et planification des créneaux.

1h

Audit

Semaine 1

Les 42 mesures du guide ANSSI sont passées en revue, point par point, avec les différents intervenant.
Il s'agit d'identifier ce qui est en place, de vérifier cette mise en place, et de déterminer ce qu'il fait défaut.
Sur une journée ou deux demi-journées.

1 journée ou 2 ½ journées

Analyse & rapport

Semaine 2

Consolidation des résultats et calcul d'un score reflétant votre niveau de sécurité.
Les mesures sont hiérarchisées selon le gain en sécurité et leur facilité de déploiement.

Livraison du rapport complet.

Restitution

Semaine 2

Réunion de présentation d'une heure, des résultats obtenus lors de l'audit, et répondre aux différentes questions que vous pouvez avoir.
Chaque recommandation est expliquée de manière concrète et adaptée à votre contexte.

2h ou plus

C – Accompagnement de mise en place

1	**Accompagnement personnalisé**	Interlocuteur sécurité pendant toute la mise en place. Avancement sur les actions avec un appui disponible à chaque étape.
2	**Coordination**	Pilotage des actions, coordination avec vos équipes ou prestataires techniques selon votre organisation.
3	**Vérification continue**	Contrôle que ce qui est mis en place couvre réellement les risques identifiés.
4	**Conditions**	Disponible après l'Offre B. Engagement mensuel, sans durée minimale imposée. Tarif journalier fixe (700 € / jour HT), volume sur devis selon la charge.

Résumé des offres

A – Etude de périmètre

Identification de vos actifs critiques (données, processus, outils) et des composants techniques qui les sous-tendent.
Vue d'ensemble des parties prenantes et les normes applicables.
Restitution claire et accessible.

950 € HT

B – Audit de sécurité

Audit basé sur le guide d'hygiène de l'ANSSI en 42 mesures, contextualisé selon vos enjeux spécifiques.
Analyse des écarts et plan d'action classé selon le gain en sécurité et la complexité de mise en œuvre.

2200 € HT

C – Accompagnement

Pilotage de la mise en œuvre des mesures de sécurité retenues.
Suivi des jalons, vérification de la couverture effective des risques et ajustement continu du plan.

Forfait à définir post plan d'action

Jean PINEAU

Consultant GRC Cybersécurité

Votre interlocuteur

Ingénieur, spécialisé en cybersécurité.

3 ans de conseil GRC chez Atos / Eviden (Paris), interventions chez divers clients : étatique, bancaire, immobilier, industriel.

- Certifié ISO 27001 Lead Auditor & Lead Implementer
- Certifié EBIOS Risk Manager

Interventions au forfait, avec un périmètre et des livrables définis en amont.

Basé en Île-de-France. Interventions à distance ou sur site.

Échangeons sur votre situation

Cliquer pour prendre rendez vous

Un premier échange de 30 minutes pour évaluer vos enjeux, sans engagement.

Jean Pineau — Consultant GRC Cybersécurité

jeanpineau@cybergrc.fr