olmen.
CONSEIL

Remise en ordre cyber

pour les industriels

Cybersécurité des entreprises jusqu'à 49 salariés.

Les comptes **La sauvegarde** **Les virements** **L'atelier**

Julien Béquet
Olmen Conseil, Nantes

07 49 86 96 07
contact@olmenconseil.fr · olmenconseil.fr

L'ESSENTIEL

« Mon prestataire s'en occupe… je crois. »

Un dirigeant, à propos de la sécurité de son informatique.

Cette fois, c'est vérifié.

Mots de passe, accès, sauvegarde, faux virements, atelier : **traités avec votre prestataire, sans arrêter la production.**

4 piliers
les comptes, la sauvegarde, les virements, l'atelier

3 à 6 mois
une demi-journée tous les 15 jours, calée sur votre production

1 interlocuteur
du cadrage à la remise

600 € HT
la demi-journée, dans un plafond fixé au devis

POUR QUI

Vous dirigez une entreprise industrielle de moins de 50 salariés. Un prestataire assure l'exploitation de votre informatique. **Personne ne pilote la cybersécurité.**

LE PRINCIPE

Je fixe les exigences de sécurité et je pilote leur mise en œuvre. Vous arbitrez. Votre prestataire réalise. **Je vérifie que c'est fait.**

DANS CE DOCUMENT

3 À quoi ressemble une mauvaise cyber ?
4 Quand faire appel à moi ?
5 Mon prestataire ne s'en occupe-t-il pas déjà ?
6 Que vérifie-t-on exactement ?
10 Comment se déroule la mission ?
11 Que me reste-t-il à la fin ?
12 Combien cela coûte-t-il ?
13 Vos questions, et qui je suis
14 Annexe technique : le socle de la mission

POURQUOI EN PARLER

Une mauvaise cyber, ça se voit.

Une cyberattaque bloque les ordinateurs et les serveurs de l'entreprise. Dans une usine, les effets sont immédiats.

Plus de commandes

L'ERP et la messagerie ne répondent plus.

Plus d'ordres de fabrication

L'atelier ne sait plus quoi produire.

Plus de livraisons

La production s'arrête, et vos clients attendent.

DANS L'ATELIER

Un vieux PC connecté à Internet.
Ses failles de sécurité ne sont plus corrigées.

Un mot de passe sur un post-it, sur la machine.
Toute personne de passage peut se connecter.

Une session ouverte en permanence, partagée par l'équipe.
Personne ne sait qui a fait quoi.

Une box 4G posée sur une machine par le constructeur.
Une connexion à Internet que personne ne surveille.

N'importe quelle clé USB branchée sur la machine.
Un virus passe ainsi du bureau à l'atelier.

DANS L'ENTREPRISE

Le constructeur se connecte à distance, personne ne sait quand.
Un accès extérieur que personne ne contrôle.

Personne ne sait qui détient les mots de passe administrateur.
Au départ de cette personne, l'accès aux outils est perdu.

Le compte d'un ancien salarié fonctionne encore.
Une personne partie conserve son accès.

La sauvegarde n'a jamais été testée.
Personne ne sait si les données peuvent être restaurées.

« Le prestataire gère », sans savoir ce qu'il fait.
Le dirigeant ne dispose d'aucune preuve.

VOUS RECONNAISSEZ UN DE CES SIGNES ?

C'est le bon moment pour en parler. Un premier échange de 30 minutes suffit à examiner votre situation.

QUAND FAIRE APPEL À MOI

Trois moments où il faut vérifier.

Chez les industriels, la cybersécurité n'a généralement pas de responsable désigné. Trois situations exposent directement l'activité.

MOMENT 1

Un changement de prestataire, ou le départ de votre informaticien

On change de prestataire à la fin du mois.

Les accès administrateur, les mots de passe et le fonctionnement des sauvegardes sont maîtrisés par **une seule personne ou un seul prestataire**.

À son départ, plus personne ne peut garantir le redémarrage de l'informatique.

MOMENT 2

Un nouveau projet : ERP, machine, ligne de production, site

Le constructeur demande un accès à distance à la nouvelle machine.

Les accès à distance de l'éditeur ou du constructeur, l'hébergement et la sauvegarde **se négocient avant la signature**. Après, chaque exigence de sécurité devient un avenant.

La sécurité est souvent supposée prise en charge par l'intégrateur, sans que personne ne l'ait vérifié. Un projet est aussi le moment où l'état réel de l'informatique apparaît.

MOMENT 3

Une cyberattaque chez un voisin, un sous-traitant ou un fournisseur

Notre fournisseur est à l'arrêt depuis une semaine.

Votre entreprise partage souvent avec ce partenaire des logiciels, des prestataires et des échanges de fichiers. **La faille exploitée chez lui peut exister chez vous.**

L'enjeu : le vérifier avant un arrêt de votre production.

⚠ **Une cyberattaque en cours chez vous ?** Contactez votre prestataire, votre assureur et le 17Cyber, dispositif public d'assistance. Je n'interviens pas pendant l'attaque. La remise en ordre commence une fois l'incident traité.

QUI FAIT QUOI

Votre prestataire réalise. Je pilote et je vérifie.

Votre prestataire assure l'exploitation de votre informatique et applique des mesures de sécurité. Le pilotage et le contrôle de ces mesures ne sont confiés à personne. Je ne le remplace pas : il conserve son rôle et ses accès.

Je fixe
ce qui doit être obtenu

→

Vous arbitrez
les priorités de l'entreprise

→

Le prestataire réalise
ou l'intégrateur, avec ses propres méthodes

→

Je vérifie
ce qui est fait, et je relance ce qui est bloqué

Et si personne ne peut réaliser une action essentielle ?

Je l'applique moi-même, avec votre accord écrit.

- ✓ J'utilise un compte administrateur temporaire, que vous supprimez à la fin de la mission.
- ✓ Votre prestataire en est informé par écrit le jour même.

Je n'interviens jamais sur un équipement livré par un constructeur : **seul le constructeur le modifie.**

Un cadre clair pour votre prestataire

- ✓ **Au cadrage**, vous présentez la mission à votre prestataire par un message préparé, moi en copie.
- ✓ **Chaque demande est écrite** et rattachée au socle en annexe. Votre prestataire peut la contester. Vous arbitrez.
- ✓ **Aucun mot de passe** n'est conservé par moi, ni transmis par mail ou par SMS.

Le but n'est pas de mettre votre prestataire en cause. Si un écart apparaît, c'est vous qui décidez de la suite.

PILIER 1 · LES COMPTES

Vos accès appartiennent à l'entreprise.

Qui a accès à quoi, avec quel mot de passe. C'est le premier point d'entrée d'une cyberattaque.

Paul est parti en mars. Son compte ? Je ne sais pas.

LES ACCÈS

- **Les comptes des personnes parties sont bloqués.**
- **Les accès administrateur** sont détenus par l'entreprise, distincts de ceux du prestataire.
- **Chaque compte est nominatif.** Personne ne travaille au quotidien avec un compte administrateur.
- **Une procédure** pour chaque arrivée et chaque départ.

LES MOTS DE PASSE

- **Un gestionnaire de mots de passe** pour toute l'équipe.
- **La double authentification** imposée sur la messagerie, les accès à distance et l'administration.

LES POSTES

- **Les mises à jour et l'antivirus** sont demandés à votre prestataire, et leurs alertes sont traitées.

CONSTATÉ À LA REMISE

Ce que vous vérifiez

- Aucun compte actif d'une personne partie.
- Votre entreprise détient les accès administrateur de ses outils.
- Aucun compte de travail administrateur.
- La double authentification est imposée.

PILIER 2 · LA SAUVEGARDE

Vos données sont restaurées devant vous.

Savoir que votre activité peut repartir, et non le supposer.

Sauvegarde : normalement, ça marche. !

LA RÈGLE

- **Le responsable de votre sauvegarde répond par écrit** : ce qui est sauvegardé, s'il existe une copie hors ligne, si la sauvegarde a ses propres identifiants.
- **Une règle de sauvegarde écrite** : quoi, quand, où, combien de temps.

CE QUI EST SAUVEGARDÉ

- **L'ERP, les serveurs et les données en ligne**, avec une copie hors ligne. S'il manque une sauvegarde, l'option est chiffrée et vous décidez.
- **Les programmes, les recettes et les réglages des machines**, avec une copie hors ligne. Sans eux, une panne peut arrêter une machine plusieurs jours.

LA REPRISE

- **Le test de restauration** est calé sur votre production.
- **Une organisation sans informatique** est prévue pendant plusieurs jours : commandes, livraisons, factures.

CONSTATÉ À LA REMISE

Ce que vous vérifiez

- ✓ Vos données sont restaurées devant vous.
- ✓ Le temps de restauration est mesuré.
- ✓ Les programmes des machines ont une copie hors ligne, ou sont notés comme demandés avec leur date.

PILIER 3 · LES VIREMENTS

Un RIB ne change jamais par mail.

La fraude au RIB joue dans les deux sens : sur vos paiements et sur vos encaissements.

VOS PAIEMENTS

« Nous changeons de banque, voici notre nouveau RIB. »

Un fraudeur écrit au nom d'un de vos fournisseurs. Le virement part sur son compte.

- **La règle ci-dessous**, expliquée à la personne qui paie.
- **La validation de chaque virement** par une seconde personne.

VOS ENCAISSEMENTS

« Merci de régler la facture sur ce nouveau compte. »

Un fraudeur écrit à vos clients en votre nom. Leur paiement part sur son compte.

- **Une mention sur vos factures** : votre RIB ne change jamais par mail.
- **Votre messagerie protégée** (pilier 1) : ces messages proviennent souvent d'une boîte mail piratée.

LA RÈGLE, POUR LA PERSONNE QUI PAIE

Tout changement de coordonnées bancaires se vérifie par un appel au fournisseur, sur un numéro déjà connu. Jamais celui du message reçu.

Toute l'équipe est sensibilisée, opérateurs compris : faux virements, hameçonnage, clés USB, et à qui signaler une anomalie.

CONSTATÉ À LA REMISE

Ce que vous vérifiez

- La règle est écrite, remise et expliquée à la personne qui paie.
- La mention est ajoutée sur vos factures.
- L'équipe est sensibilisée.

PILIER 4 · L'ATELIER

Chaque machine et chaque accès ont un responsable.

Les postes, les machines et les accès à distance ne figurent souvent dans le contrat de personne.

Le PC de la ligne 2 ? Personne n'y touche depuis des années.

CONNAÎTRE

- **La liste des machines, des automates et des PC d'atelier**, de leurs accès à distance et de leur constructeur.

SÉPARER

- **L'atelier est séparé du bureau par un pare-feu.** Aucun accès direct depuis Internet.

ENCADRER

- **La télémaintenance est fermée par défaut**, ouverte à la demande, avec un compte par personne.
- **Les mots de passe par défaut** des automates et des écrans sont changés.

CONSTATÉ À LA REMISE

Ce que vous vérifiez

- Chaque poste d'atelier est recensé et a un responsable.
- Chaque accès à distance, des postes de bureau aux machines de l'atelier, a un responsable identifié.
- La séparation entre bureau et atelier est réalisée, ou notée comme demandée avec sa date.

LA RÈGLE, À L'ATELIER

Je ne modifie jamais ce qu'un constructeur ou un intégrateur a livré et validé : automates et programmes, IHM, PC fournis avec les machines, supervision. Je prescris. Le constructeur valide et exécute.

LE DÉROULÉ

Une demi-journée tous les 15 jours, pendant 3 à 6 mois.

Entre deux rendez-vous, vos intervenants réalisent les actions.

LE DÉMARRAGE rendez-vous rapprochés

Cadrage — **Comprendre l'entreprise** — Dirigeant

Sur site, avec vous : ce qui ne doit jamais s'arrêter, vos outils, vos intervenants, un premier tour de l'atelier.

Devis — **Fixer le plafond de demi-journées** — Dirigeant

Visite — **Voir en détail les bureaux et l'atelier** — Équipe

Les postes, les machines, les accès à distance. Vos prestataires répondent par écrit à mes questions.

Arbitrage — **Décider des priorités** — Dirigeant

Les exigences, le travail de chaque intervenant et son coût. Vous décidez de ce qui est réalisé.

LE PILOTAGE environ tous les 15 jours

Pilotage — **Faire avancer les actions** — Intervenants

Un point avec le prestataire, l'intégrateur ou le constructeur. Je vérifie ce qui est fait, je relance ce qui est bloqué. Le dossier informatique se complète au fil des rendez-vous.

une demi-journée — **Former l'équipe, opérateurs compris** — Équipe

une demi-journée — **Restaurer vos données devant vous** — Dirigeant, prestataire

LA FIN quand chacun des points a été traité

Remise — **Constater le résultat** — Dirigeant

Je vous remets la page de résultat et le dossier informatique. Vous supprimez mes accès.

Un mois après — **Le contrôle** — Dirigeant

Un appel : ce qui tient, ce qui reste demandé.

VOTRE TEMPS

Le cadrage, l'arbitrage, la restauration et la remise. Le calendrier est calé sur votre production et sur la disponibilité de vos équipes.

LE PÉRIMÈTRE

Ce que vous gardez

À la remise, ces éléments vous appartiennent. Ils restent en place après mon départ.

Votre entreprise est propriétaire

Des accès administrateur, des abonnements, du nom de domaine.

Le prestataire assure l'exploitation

De vos outils au quotidien, comme aujourd'hui.

Je pilote et je vérifie

Jusqu'à la remise, puis le contrôle à 30 jours.

Ce qui vous est remis

La page de résultat

- ✓ Ce qui est vérifié, pilier par pilier
- ✓ Sa date et le document qui le prouve
- ✓ Ce qui reste demandé, à qui, depuis quand

Le dossier informatique

Il appartient à l'entreprise. Je n'en garde pas de copie.

EN CAS D'INCIDENT

La fiche réflexe
les premiers gestes, qui appeler

Isoler l'atelier
du bureau et des accès à distance

Vos intervenants
leurs contacts, leur rôle

AU QUOTIDIEN

L'inventaire
postes, machines, accès à distance

Les accès administrateur
où les trouver, sans mot de passe

Vos règles écrites
sauvegarde, virements, arrivées et départs

LES PREUVES

Chaque point vérifié
exports et captures, datés

La restauration
son compte rendu, avec la durée

Les réponses écrites
de chaque intervenant

Ce qui n'est pas compris

- ✕ Le support informatique au quotidien.
- ✕ L'intervention pendant une cyberattaque.
- ✕ La fonction permanente de responsable de la sécurité.
- ✕ La vente de matériel ou de logiciel.
- ✕ Le réglage des automates et des machines.

LE PRIX

600 € HT la demi-journée.

Vous ne payez que les demi-journées réalisées, dans la limite d'un plafond fixé après le cadrage.

COMPRIS DANS LA DEMI-JOURNÉE

- ✓ La préparation et les comptes rendus
- ✓ La page de résultat et le dossier informatique
- ✓ Les quatre piliers, traités et vérifiés
- ✓ Les déplacements en Loire-Atlantique
- ✓ Le pilotage de vos intervenants
- ✓ L'appel de contrôle, un mois après la remise

Un exemple, pour une entreprise de 20 salariés

10	5 mois	6 000 € HT
demi-journées, cadrage compris	environ une demi-journée tous les 15 jours	environ

AIDE DE LA RÉGION

Jusqu'à 30 % pris en charge

Le dispositif Pays de la Loire Conseil couvre la cybersécurité, à partir de 5 000 € HT de dépenses. Le dossier se dépose avant tout engagement, sous réserve d'éligibilité.

À votre charge, annoncé avant de décider

Interventions de vos prestataires	Prestataire, intégrateur, constructeur. Chiffrées par écrit, validées par vous.	**Chiffrées à l'arbitrage**
Matériel et licences	Pare-feu, sauvegarde, gestionnaire de mots de passe, selon ce qui manque.	**Chiffrés à l'arbitrage, sur votre décision**

AVANT DE DÉCIDER

Vos questions

Faudra-t-il arrêter l'atelier ?

Le calendrier est calé sur votre production. Une action qui demande un arrêt est prévue sur un arrêt existant, ou arbitrée par vous.

Et si un intervenant ne répond pas ?

Les actions non réalisées figurent dans la page de résultat, avec la date de la demande. Vous décidez de la suite.

Que se passe-t-il après la mission ?

Je vous appelle un mois après la remise. La page de résultat et le dossier informatique restent à l'entreprise.

Garantissez-vous l'absence de cyberattaque ?

Non, aucun prestataire ne le peut. Je m'engage à ce que chaque point soit traité, ou noté comme demandé avec sa date. Chaque point traité est vérifié, avec sa preuve.

Aurez-vous accès à nos données ?

Un accès en lecture à la configuration, pas au contenu de vos mails ni de vos fichiers. Vous supprimez mes accès vous-même, à la remise.

Et en cas d'incident pendant la mission ?

La mission est suspendue, le temps de traiter l'incident. Je vous oriente vers le 17Cyber, dispositif public d'assistance.

Et si la mission prend plus de temps ?

Le plafond est fixé au départ. Si je me trompe, vous ne payez pas plus. Si un intervenant prend du retard, vous décidez de la suite.

ET MAINTENANT

1. **Un premier échange de 30 minutes**
   sans engagement, pour examiner votre situation.
2. **Le cadrage**
   une demi-journée facturée seule.
3. **Le devis**
   avec le plafond.

Appelez-moi au 07 49 86 96 07.

Vous accompagnez des industriels ? Si vous voyez un des signes de la page 3, appelez-moi.



Julien Béquet
Consultant en cybersécurité

Olmen Conseil, conseil en cybersécurité à Nantes. J'interviens dans votre entreprise, avec votre prestataire informatique.

Indépendant : je n'ai aucun matériel, logiciel ou contrat d'infogérance à vendre. Mes exigences sont établies d'après les guides publics de l'ANSSI.

07 49 86 96 07
contact@olmenconseil.fr
olmenconseil.fr

ANNEXE TECHNIQUE

Le socle de la mission

Les mesures que la mission traite, d'après deux guides de l'ANSSI. Elles empêchent qu'un incident courant ne devienne un arrêt de l'activité. Chaque point est fait et prouvé, noté comme demandé, ou sans objet avec sa raison.

	TOUTE L'ENTREPRISE	INFORMATIQUE DE GESTION	INFORMATIQUE DE PRODUCTION
Connaître	Chacun sait à qui s'adresser en cas de doute. HYG 39 Un référent désigné ; les activités et données à protéger en priorité, validées par la direction. HYG 39 · HYG 4 · R1 Qui fait quoi, par écrit : direction, prestataire, constructeurs. R2 · HYG 3 Comptes à privilèges et prestataires ayant un accès, inventoriés. HYG 5 · HYG 3 · R4	Inventaire du parc : postes, serveurs, logiciels, abonnements en ligne. HYG 4	Liste des machines, automates et PC d'atelier, de leurs accès à distance et de leur constructeur. R4 · R5
Protéger	Sensibilisation régulière de tous, opérateurs compris : hameçonnage, faux virements, clés USB, avec une clé dédiée à l'atelier. HYG 2 · R174 · R175 Changement de RIB vérifié par rappel ; virement validé par une seconde personne. Bonne pratique Comptes fermés et accès retirés au départ, au bureau comme à l'atelier. HYG 6 · R86	Mises à jour systématiques ; antivirus sur tous les postes. HYG 14 · HYG 34 Double authentification : messagerie, accès à distance, administration ; aucun accès d'administration ouvert sur Internet. HYG 13 · HYG 32 · HYG 23 Comptes nominatifs, pas d'administrateur au quotidien, mots de passe robustes. HYG 8 à 12 · HYG 29	Atelier séparé du bureau par un pare-feu ; aucun accès direct depuis Internet. R101 à R103 · R116 à R118 · R122 · R123 · R125 Télémaintenance fermée par défaut, ouverte à la demande, un compte par personne. R83 · R84 · R124 · R129 Mots de passe par défaut des automates et des écrans changés ; comptes partagés de l'atelier rattachés à un responsable. R87 · R84 · R83–
Détecter	Signaler immédiatement toute anomalie, sans crainte de sanction. HYG 2 · HYG 40	Alertes de l'antivirus et des services en ligne activées, et traitées. HYG 14	
Réagir	Premiers gestes connus de tous : débrancher du réseau sans éteindre, prévenir. HYG 40 Fiche réflexe : qui appeler, porter plainte, prévenir la CNIL sous 72 h si besoin. HYG 40 · RGPD art. 33	Isoler le poste ou le compte touché ; changer les mots de passe exposés. HYG 40	Savoir isoler l'atelier du bureau et de la télémaintenance, en sachant quelles machines continuent de fonctionner. R77 · R116
Repartir	Savoir travailler sans informatique plusieurs jours : commandes, livraisons, factures. R74 Règle de sauvegarde écrite : quoi, quand, où, combien de temps. HYG 37 · R8 · R73	Sauvegardes régulières, données en ligne comprises, avec une copie hors ligne ; restauration testée. HYG 14 renforcé · HYG 37	Programmes, recettes et réglages des machines sauvegardés à chaque modification, copie hors ligne. R8 à R11

HYG : Guide d'hygiène informatique (ANSSI, 2017). R : La cybersécurité des systèmes industriels, Mesures détaillées (ANSSI, 2025). Quelques bonnes pratiques les complètent, dont la vérification des virements.