

1 · SYNTHÈSE

Extrait de rapport Ekera — Ateliers Morvan (exemple fictif)

Diagnostic Ekera d'une ETI industrielle fictive de 420 salariés, établi à partir de ses documents, de ses exports et d'un entretien, sans accès direct à son système d'information.

81 % de l'activité critique arrêtée dans le pire scénario d'attaque

INDICATEUR	SITUATION DE RÉFÉRENCE	APRÈS TRAVAUX (SIMULATION)
Arrêt maximal après une attaque	81 %	34 %
Pire scénario	2,4 à 4,9 M€	0,9 à 1,8 M€
Perte annuelle attendue	150 à 980 k€	40 à 260 k€
Portes d'entrée faibles	5	1
Sauvegardes hors d'atteinte	non	oui
Mesures NIS2 évaluées satisfaites	4,5 sur 10	8 sur 10

Ce qui a été lu

- Huit sources : documents (schémas, contrats, procédures), inventaire GLPI, annuaire, pare-feu, tickets des 12 derniers mois, logiciel d'achat, Microsoft 365, console cloud
- La carte obtenue : 23 applications, 38 serveurs, 41 flux, 7 fournisseurs ; les doublons entre sources sont fusionnés
- Un entretien de trois questions avec le DSI, sur ce que les sources ne disaient pas

À revoir en priorité

Point unique de défaillance sur les expéditions

Continuité · source : inventaire, entretien

Infogérant connecté en permanence

Fournisseurs · source : annuaire, connecté 212 jours sur 365

Restauration de sauvegarde jamais testée

Sauvegardes · source : entretien, tickets

Comptes à privilèges partagés

Accès · source : annuaire

Aucune procédure de déclaration d'incident sous 24 h

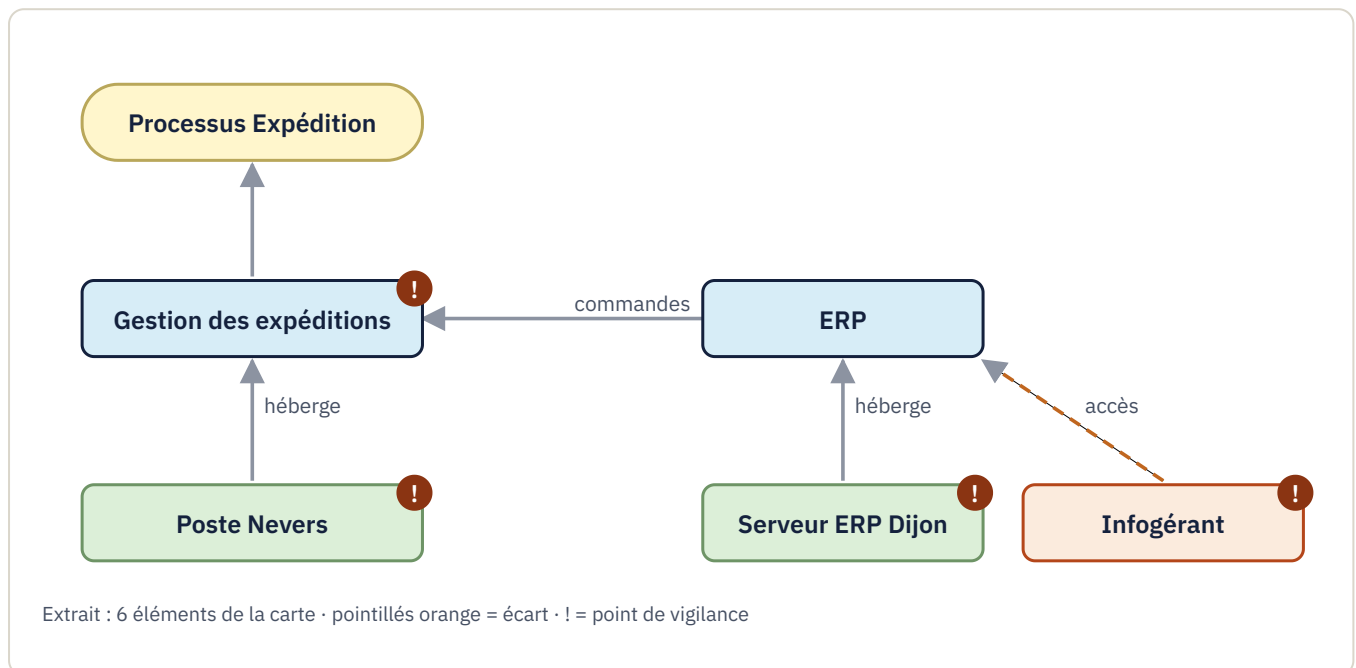
Incidents · source : procédures

« Après travaux » : estimations conditionnelles, qui supposent les mesures réalisées et produisant les effets modélisés ; pas des réductions de risque garanties. Le score NIS2 compte les dix mesures de l'article 21 (1 point par mesure satisfait, ½ si partielle) ; il ne constitue pas une attestation de conformité.

2 · CARTOGRAPHIE D'UNE DÉPENDANCE CRITIQUE

L'expédition dépend d'un seul poste, à Nevers

Le contrat de maintenance cite un logiciel de gestion des expéditions, absent de l'inventaire. L'entretien a établi où il tourne : la carte en fait un point unique de défaillance, c'est-à-dire un élément dont la panne peut à elle seule interrompre une activité critique.



La question de l'entretien

« Le contrat de maintenance cite un logiciel de gestion des expéditions, absent de l'inventaire. Où tourne-t-il ? »
Réponse du DSI : « Sur un seul poste, à l'entrepôt de Nevers. »

ÉLÉMENT	TYPE	HÉBERGEMENT	CRITICITÉ	ÉCART	SOURCES
Gestion des expéditions	Application	Poste de Nevers	Haute	Absente de l'inventaire ; point unique de défaillance, aucune sauvegarde déclarée	Contrat de maintenance, entretien
Poste Nevers	Poste de travail	Entrepôt de Nevers	Haute	Héberge seul une application critique	Inventaire GLPI, entretien
ERP	Application	Serveur ERP Dijon	Haute	Version proche de la fin de support (2027)	Inventaire GLPI, contrat éditeur, pare-feu
Serveur ERP Dijon	Serveur	Salle serveur Dijon	Haute	Restauration jamais testée	Inventaire GLPI, console cloud
Infogérant	Fournisseur	Prestataire externe	Haute	Accès permanent, sans bastion ni clause de sécurité	Annuaire, factures, entretien

Chaque fait cite sa source : dépendance, contrat de maintenance, p. 4 ; absence de sauvegarde, rapport de sauvegarde du 3 octobre.

3 · SCÉNARIO D'INCIDENT ET HYPOTHÈSES FINANCIÈRES

Que coûterait un arrêt de l'ERP pendant 3 jours ?

La question que le DSI des Ateliers Morvan pose à la carte, en français. Les chiffres viennent du moteur de calcul d'Eker, indépendant du modèle de langage : mêmes données, même résultat.

Ce que l'ERP porte · 6 processus, dont la facturation et les expéditions

Coût du scénario : arrêt de l'ERP pendant 3 jours · 0,6 à 1,1 M€

D'où viennent les chiffres · Moteur Eker, hypothèses affichées · ERP : inventaire GLPI · chiffre d'affaires : fichier des écritures comptables 2025

Quatre notions à distinguer

NOTION	ATELIERS MORVAN	CE QU'ELLE MESURE
Coût d'un scénario : le pire scénario	2,4 à 4,9 M€	La perte de la porte d'entrée la plus coûteuse
Coût d'un scénario : arrêt de l'ERP pendant 3 jours	0,6 à 1,1 M€	Ce que coûterait cet incident donné, selon sa durée et son périmètre
Perte annuelle attendue	150 à 980 k€	Ce que les scénarios étudiés coûteraient en moyenne chaque année
Effet des mesures : arrêt maximal après une attaque	81 % → 34 %	Une variation de risque modélisée, pas une dépense évitée

Les hypothèses de calcul

- Perte annuelle attendue : pour chaque porte d'entrée et chaque point unique de défaillance, fréquence annuelle estimée × perte du scénario, additionnées.
- Fourchettes : des hypothèses basses (fréquences, jours d'arrêt, coûts de réponse) aux hautes.
- Comptes : le fichier des écritures comptables donne le chiffre d'affaires et les charges variables ; la marge est répartie entre les flux de revenu, chacun compté une fois.
- Arrêt : un processus compte comme arrêté dès qu'un composant dont il dépend est atteint ; le moteur ne distingue pas les processus seulement dégradés.

Des estimations en fourchettes, à discuter avec les équipes techniques et financières : une base argumentée pour prioriser, pas une garantie du coût réel d'un futur incident. Reproductible ne veut pas dire exact : le résultat vaut ce que valent les données et les hypothèses.

4 · COMPARAISON DE TROIS VARIANTES DE TRAVAUX

Continuité des expéditions : trois solutions évaluées

Pourquoi : fin de support du logiciel d’expédition annoncée pour juin 2027, incidents répétés, exigence NIS2 de continuité non tenue. Méthode : deux critères éliminatoires, puis cinq familles de critères pondérées.

VARIANTE	DESCRIPTION	NOTE	APPRÉCIATION
A	Garder le logiciel actuel, ajouter un poste de secours	Éliminée	Pas d’authentification nominative, critère éliminatoire
B	Module logistique de l’ERP SaaS européen	82 / 100	Recommandée : continuité, intégration, cybersécurité
C	Logiciel de transport tiers	70 / 100	Bonne couverture, un fournisseur de plus

La variante B, prête pour la demande de devis

- Quantités lues dans les outils : module logistique de l’ERP, 1 entrepôt, 6 utilisateurs, 1 interface avec l’ERP
- Clauses à mettre au contrat : hébergement dans l’UE, journaux transmis, réversibilité, notification d’incident sous 24 h
- Ordre de grandeur du catalogue : 38 à 55 k€, à confirmer par devis

Décision enregistrée en brouillon : ADR-009, solution B retenue. Critères, notes, sources et solutions écartées sont conservés. Elle passe dans le circuit de décision, puis sera écrite dans Archi. Les achats valident et envoient la demande de devis ; Eker ne passe jamais de commande.

Effet modélisé de l’ensemble des travaux (simulation)

Arrêt maximal après une attaque · 81 → 34 %



Mesures NIS2 évaluées satisfaites · 4,5 → 8 sur 10



■ référence · ■ après travaux

Résultats « après travaux » : estimations conditionnelles. Les coûts sont des ordres de grandeur, remplacés par les devis puis par les factures.

5 · FEUILLE DE ROUTE PRIORISÉE

Les chantiers, dans l'ordre

Les chantiers découlent des écarts. Charges en jours : des ordres de grandeur tirés du catalogue de briques, à confirmer par devis.

CE TRIMESTRE	PREMIER SEMESTRE 2027	SECOND SEMESTRE 2027
Sauvegarde et secours du poste d'expédition Continuité · 3 j	Plan de continuité des expéditions Continuité · 6 j	Clauses de sécurité dans les contrats fournisseurs Conformité · 4 j
Comptes nominatifs, double authentification Accès · 8 j	Cloisonnement réseau, portail fournisseurs Sécurité · 12 j	Remplacement du pare-feu de Dijon Obsolescence · 5 j
Procédure de déclaration d'incident Incidents · 2 j	Test de restauration, puis chaque trimestre Sauvegardes · à chiffrer	Retrait de l'outil de devis, licences inutiles Coûts · 2 j
Accès de l'infogérant par bastion Fournisseurs · à chiffrer		Décision puis migration de l'ERP Obsolescence · à chiffrer

Le circuit de décision

DSI · RSSI · Directeur financier · Achats · Direction générale

Chacun approuve, refuse ou demande une modification ; les décisions et les avis sont tracés. Rien n'est écrit dans les outils de l'entreprise avant la validation d'une personne habilitée, et chaque écriture se défait.

Ensuite, le suivi continu

Ekera croise l'extérieur et les outils avec la carte : faille publiée sur la version de l'ERP, serveur absent de la carte, fin de support du logiciel d'expédition (juin 2027), nouvelle version du Référentiel Cyber France. Il alerte sur ce qui touche l'entreprise et propose les évolutions à décider.