Acronis

LIVRE BLANC

Pourquoi les fabricants européens ont besoin d'un plan de résilience pour leurs entreprises

Réduire les interruptions d'activité, soutenir la préparation à NIS 2 et améliorer l'éligibilité aux cyberassurances

Résumé

Les fabricants européens font face à une confluence de défis :

L'interruption d'activité imprévue figure parmi les menaces les plus importantes en termes de dégradation des performances sur le secteur de la fabrication à l'échelle de tout le continent.

L'évolution continue de la directive NIS 2 fait que la continuité des activités et la reprise après sinistre relèvent désormais de la responsabilité de la direction générale.

Dans le même temps, les cyberassureurs exigent des preuves de résilience plus strictes avant de valider la souscription.

Le problème est que ces pressions ne sont plus distinctes. Aujourd'hui, un seul incident de cybersécurité ou sinistre a un impact direct sur les opérations, la conformité et le rétablissement financier. Dans ce contexte, les fabricants doivent dépasser les stratégies de sauvegarde fragmentées pour leurs environnements de technologies opérationnelles (OT) et adopter un véritable plan de résilience d'entreprise axé sur le rétablissement de la production.

Le défi pour la direction : un incident, trois impacts

De nombreuses organisations gèrent encore séparément la sauvegarde, la conformité et la police d'assurance. En théorie, ces pratiques convergent lors d'un incident. Mais que se passe-t-il si ce n'est pas le cas ?

Si un fabricant ne peut pas rétablir sa production de manière contrôlée et documentée, il s'expose à trois conséquences immédiates :

- Perturbation de la production et engagements de livraison non tenus.
- Exposition réglementaire au titre de NIS 2.
- Risque accru de déclarations de sinistres contestées ou revues à la baisse.

Une capacité de restauration insuffisante crée donc un risque accru pour l'entreprise, et pas seulement un problème technique.

Paysage des menaces en Europe et situation par région

Les cyberincidents perturbent déjà les opérations de fabrication en Europe, le ransomware restant la menace principale pour les environnements industriels. Les fabricants européens font face à des risques convergents. Les gangs de ransomware ciblent le secteur manufacturier, avec un nombre accru d'incidents graves et une plus large exposition aux vulnérabilités. Parralèlement, de nombreuses petites et moyennes entreprises (PME), y compris des fabricants, ne disposent pas de stratégies de cybersécurité matures et sont donc vulnérables aux attaques. Les initiatives portées par l'Industrie 4.0 ont également élargi la surface d'attaque des environnements OT, or de nombreux fabricants n'ont pas pris de mesures adéquates pour protéger leurs données.

Se remettre d'une cyberattaque coûte cher. À l'échelle mondiale, le coût moyen d'une violation de données dans un environnement industriel s'élevait à 5,0 millions de dollars en 2025, selon IBM.[1] Avec la hausse du nombre et de la gravité des attaques de ransomware et d'autres attaques en Europe, les fabricants, comme les autres PME, doivent élaborer une stratégie de protection et de restauration efficace. Les chiffres suggèrent que la situation s'aggrave, et non le contraire.

Par exemple :

Europe : selon le rapport ENISA Threat Landscape 2025, près de 15 % des attaques de ransomware analysées visaient le secteur manufacturier, soit le cinquième secteur le plus ciblé parmi près de 20 secteurs étudiés dans le rapport.[2]

Royaume-Uni : le National Cyber Security Centre (NCSC) indique que le secteur manufacturier figure parmi les secteurs les plus fréquemment ciblés par les attaques de ransomware.[3]

Allemagne : Any.run a indiqué en 2026 qu'en raison de l'intégration par les fabricants allemands des technologies de l'Industrie 4.0, des capteurs IoT, de l'OT opérationnelle et de systèmes de production intégrés au cloud, les attaques provoquaient plus que la perte de données et pouvaient entraîner un arrêt total, des dommages matériels physiques et des perturbations de la chaîne d'approvisionnement. Et comme le personnel en atelier était rarement formé à la cybersécurité, les attaques d'ingénierie sociale se sont avérées particulièrement efficaces.[4]

France : l'agence française de cybersécurité (ANSSI) a indiqué dans un rapport de 2026 que les fabricants français étaient devenus des cibles majeures tant pour les perturbations liées à des ingérences étrangères que pour les attaques de ransomware. Le rapport précisait que les plus petits fabricants étaient particulièrement vulnérables au sabotage numérique.[5]

Italie : un rapport de cybersécurité de Telecom Italia a révélé en 2025 que les entreprises manufacturières italiennes avaient été la cible d'environ 26 % des attaques de ransomware dans le pays entre 2022 et 2024.[6]

Pays nordiques : Mordor Intelligence indique que les programmes Industrie 4.0 qui étendent les surfaces d'attaque OT stimulent les investissements dans les solutions de cybersécurité dans les pays nordiques, avec un taux de croissance annuel composé (TCAC) impressionnant de plus de 8 % par an. Les fabricants répondent aux risques en faisant converger les défenses IT et OT.[7]

Bien que les statistiques spécifiques à l'OT restent limitées, les données nationales disponibles mettent en évidence l'intensification plus large du cyberrisque dans les environnements de fabrication, y compris les systèmes industriels et les PME.

[1] IBM, Cost of a Data Breach Report 2025: The AI Oversight Gap, recherche menée par Ponemon Institute, publiée en 2025, sur la base de l'analyse de 600 organisations dans 16 pays entre mars 2024 et février 2025.

[2] ENISA Threat Landscape 2025, version 1.2, Agence de l'Union européenne pour la cybersécurité, janvier 2026.

[3] National Cyber Security Centre. (2024). Revue annuelle 2024 du NCSC. GCHQ.

[4] ANY.RUN. (1er avril 2026). Principales cyberattaques en mars 2026 : phishing OAuth, contrebande SVG, Magecart, et plus encore.

[5] Agence nationale de la sécurité des systèmes d'information. (11 mars 2026). Panorama de la cybermenace 2025 (CERTFR-2026-CTI-002). ANSSI.

[6] Telecom Italia (TIM), & Cyber Security Foundation. (12 juin 2025). Rapport sur la cybersécurité 2025. TIM Group.

[7] Mordor Intelligence, analyse de la taille et du partage du marché de la cybersécurité dans les pays nordiques : tendances et prévisions de croissance (2026–2031), estimant la taille du marché à 14,92 milliards de dollars en 2026, pouvant atteindre 22,25 milliards de dollars d'ici 2031 (TCAC de 8,36 %), publiée en 2026.

Cyberattaques constatées contre le secteur manufacturier en Europe

Dans toute l'Europe, les cyberincidents dans les environnements OT ne sont plus des événements informatiques isolés. Ce sont des événements de production qui peuvent gravement perturber les opérations et entraîner une interruption d'activité prolongée. Exemples récents :

- **Jaguar Land Rover :** une cyberattaque de 2025, désormais tristement célèbre, contre Jaguar Land Rover a perturbé la production au Royaume-Uni pendant plusieurs semaines, pour un coût estimé d'au moins 50 millions de livres par semaine,[8] avec des suppressions d'emplois à la clé. L'attaque a démontré comment une perturbation du système informatique d'une entreprise peut avoir un impact direct sur les opérations de fabrication.
- **Volkswagen Group France :** en octobre 2025, Volkswagen Group France a subi une attaque du gang de ransomware Qilin qui a conduit à l'exfiltration d'environ 2 000 fichiers et de 150 Go de données sensibles.[9]
- **Dodd Group :** en 2025, Dodd Group, sous-traitant britannique de défense, a subi une cyberattaque qui a provoqué la fuite de fichiers sensibles du ministère britannique de la Défense, y compris des informations sur les bases de l'armée de l'air et de la marine.[10]

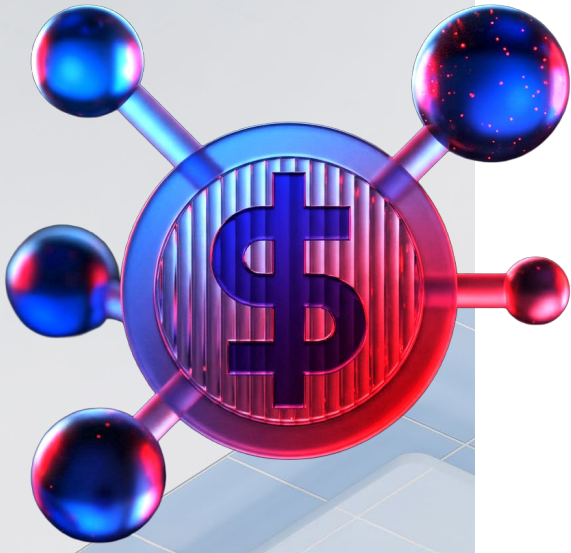
Ce que NIS 2 exige en pratique

La conformité reste un enjeu majeur dans les environnements OT, où les pénalités financières potentielles peuvent venir alourdir le coût d'une interruption d'activité imprévue. NIS 2 introduit un changement fondamental : de la prévention à une résilience démontrable.

En vertu de l'article 21, les organisations doivent être en mesure de prouver qu'elles peuvent poursuivre leurs opérations et restaurer efficacement leurs activités. Cette collecte concerne notamment les éléments suivants :

- Planification de la continuité des activités et de la reprise d'activité après sinistre.
- Gestion des sauvegardes alignée sur les besoins opérationnels.
- Structures de gestion de crise et de gouvernance.

Le changement majeur concerne la responsabilité : les organisations doivent démontrer que la restauration fonctionne dans la pratique, et pas seulement sur le papier. Ainsi, la capacité de restauration est désormais une exigence de conformité, et non une simple préférence opérationnelle.



[8] BBC News, Jaguar Land Rover cyber-attack disrupts production and supply chain, publié en septembre 2025.
[9] Cybernews. (16 octobre 2025). Volkswagen France hit by ransomware, Qilin gang claims.
[10] Security Affairs. (20 octobre 2025). Russian Lynk group leaks sensitive U.K. MoD files, including info on eight military bases.

Pourquoi la restauration OT est différente

Les environnements OT introduisent des complexités que les approches traditionnelles de restauration IT ne traitent pas entièrement, notamment les systèmes traditionnels, les processus de production étroitement couplés et les conditions strictes de redémarrage qui rendent le séquencement de la restauration critique.

Par conséquent, la résilience du secteur manufacturier dépend
de la restauration de la capacité de production, non seulement des systèmes ou des données.

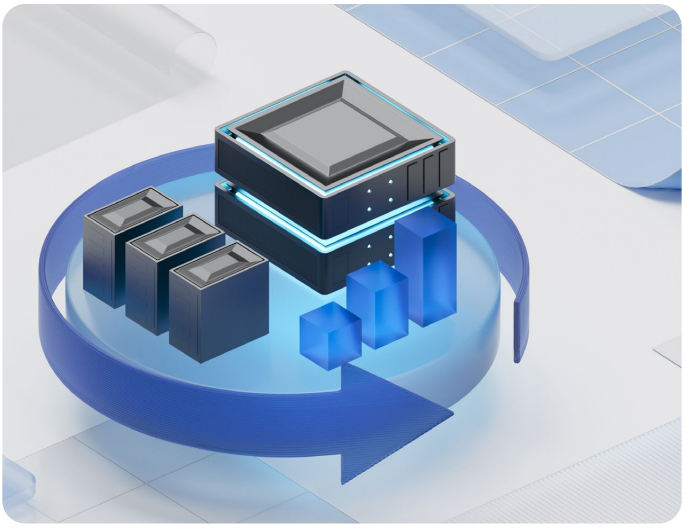
De la sauvegarde à la résilience d'entreprise

Un plan de résilience d'entreprise implique bien plus qu'une simple sauvegarde ; il relie la continuité opérationnelle, la conformité et la restauration au sein d'un même cadre.

Au minimum, les organisations devraient mettre en place :

- Une gouvernance claire des sites et des fonctions.
- Des capacités de restauration adaptées à l'OT.
- Une validation régulière des processus de restauration.

L'objectif n'est pas simplement la restauration de données, mais de garantir que les fabricants puissent restaurer la production rapidement, de manière contrôlée et prévisible.



Cyberassurance et capacité de défense

Les cyberassureurs examinent de plus en plus attentivement les organisations manufacturières, en particulier concernant le risque d'interruption d'activité. L'issue des sinistres est de plus en plus influencée par la capacité d'une organisation à démontrer sa préparation et l'exécution de sa restauration.

Les principaux critères comprennent désormais :

- Des preuves de processus définis de continuité et de restauration.
- La documentation des délais et des actions de restauration.
- L'alignement des politiques sur la capacité opérationnelle.

Sans ces éléments, les organisations risquent d'entrer dans une zone grise où la couverture de sinistre peut être réduite ou contestée.

Ce que les dirigeants du secteur manufacturier devraient faire ensuite

Les fabricants doivent davantage traiter la résilience comme une priorité d'entreprise que comme un projet technique.

Les dirigeants devraient se concentrer sur trois actions immédiates :

- Comprendre les dépendances de production critiques et les risques de restauration.
- Aligner la planification de la continuité sur les attentes de NIS 2.
- Mettre en place un plan structuré de résilience d'entreprise.

Cette évolution permet aux organisations de réduire le risque d'interruption d'activité tout en renforçant à la fois la conformité et la protection financière.

Comment Acronis soutient la résilience OT

Avec Acronis Cyber Protect pour l'OT, les systèmes peuvent être restaurés en une seule action, sans nécessiter d'expertise informatique approfondie. Dans les environnements isolés du réseau en particulier, One-Click Recovery devient essentielle. Les fabricants peuvent minimiser les interruptions d'activité et maximiser la vitesse de restauration sans intervention ni perturbation.

Acronis Cyber Protect pour l'OT permet aux fabricants de renforcer la résilience au sein d'environnements complexes. Les organisations peuvent ainsi faire converger les défis suivants :

- Protéger les systèmes critiques contre les interruptions d'activité imprévues.
- Valider les processus de restauration et les autres aspects essentiels à la conformité.
- Générer les preuves requises pour les polices de cyberassurance.

Composant de l'Acronis Cyber Platform nativement intégrée, qui combine plusieurs fonctions de cybersécurité dans une console unique avec un point de gestion unique, Acronis Cyber Protect pour l'OT permet aux fabricants d'améliorer le temps de fonctionnement et de réduire les interruptions d'activité imprévues, tout en bénéficiant de temps de restauration plus rapides et d'un meilleur alignement entre la résilience opérationnelle et la gestion des risques de l'entreprise.

EN SAVOIR PLUS

Acronis

Pour en savoir plus : acronis.com