

La sécurité de vos fournisseurs est la vôtre

Prestataire IT, logiciel métier, expert-comptable, agence : chaque fournisseur connecté est une porte vers vous. Évaluer sans inquisition.

8 min de lecture · Niveau Intermédiaire · cyberionis.fr/ressources/securite-fournisseurs

Les attaques « par la chaîne d'approvisionnement » ne visent plus que les géants : le prestataire IT compromis qui contamine tous ses clients, le logiciel métier piraté qui diffuse la charge, l'expert-comptable dont la boîte fuite vos données — les PME les subissent en cascade. NIS2 en a fait une obligation pour les entreprises régulées ; le bon sens en fait une nécessité pour toutes : votre sécurité vaut celle du moins sûr de vos fournisseurs connectés.

1. Cartographier : qui est connecté à quoi

- Lister les fournisseurs qui touchent votre numérique : accès distants (prestataire IT, mainteneurs d'équipements), logiciels et SaaS, hébergeurs, et détenteurs de vos données (comptable, paie, agence)
- Pour chacun : quel accès, quelles données, quel impact s'il tombe ou s'il est compromis — trois colonnes suffisent
- Classer en deux niveaux : les critiques (accès profond ou données sensibles) méritent l'évaluation complète ; les autres, les vérifications de base
- Cette carte rejoint le registre RGPD (sous-traitants) et l'inventaire : trois usages, un seul travail

2. Évaluer sans questionnaire de 400 lignes

- Les cinq questions qui discriminent : MFA sur leurs accès à vos systèmes ? Comptes nominatifs et journalisés ? Que se passe-t-il chez eux en cas d'incident (et vous préviennent-ils sous quel délai) ? Vos données sont-elles chiffrées et où ? Ont-ils une assurance cyber ?
- Les preuves simples : certification (ISO 27001, labels comme ExpertCyber), DPA sérieux, politique de sécurité communicable — un fournisseur mature les fournit sans friction
- Le comportement compte autant que les papiers : celui qui rechigne aux cinq questions de base en dit long
- Réévaluer à chaque renouvellement et après tout incident chez eux — l'évaluation unique de 2023 ne dit rien de 2026

ATTENTION

Le cas d'école qui se répète : l'outil de prise en main à distance du prestataire IT compromis, et tous ses clients chiffrés la même nuit. Vos questions à VOTRE prestataire sur SA sécurité (MFA sur ses outils, séparation de ses accès clients, supervision de ses propres systèmes) ne sont pas de la défiance — c'est la due diligence que les prestataires sérieux attendent, et que les autres redoutent.

3. Contractualiser l'essentiel

- La notification d'incident : le fournisseur touché vous prévient sous un délai défini (24-72 h) — sans cette clause, vous l'apprendrez par la presse
- Les exigences d'accès : MFA, comptes nominatifs, coupure en fin de contrat — écrites, pas supposées
- Le DPA pour tout traitement de données (article 28) et la localisation des données
- La réversibilité et la continuité : que se passe-t-il si le fournisseur ferme, est racheté, ou si vous partez (voir nos guides)
- Pour les petits fournisseurs sans juriste : une annexe sécurité d'une page vaut mieux que rien — et le marché s'y habitue

4. Limiter l'impact par construction

- Le moindre privilège s'applique aux fournisseurs d'abord : accès dédiés, limités, journalisés, activés à la demande
- Vos sauvegardes indépendantes des données confiées aux SaaS critiques : l'assurance contre leur défaillance
- La supervision qui voit les connexions fournisseurs : l'accès de maintenance qui se connecte un dimanche à 3 h se remarque
- Le scénario « fournisseur compromis » ajouté au plan de réponse : qui coupe quoi, qui appelle qui

L'essentiel à retenir

- 01 Cartographier les fournisseurs connectés et leurs accès
- 02 Poser les cinq questions de sécurité aux critiques
- 03 Exiger contractuellement notification d'incident et règles d'accès
- 04 Appliquer le moindre privilège aux accès fournisseurs
- 05 Garder des sauvegardes indépendantes des données confiées
- 06 Réévaluer à chaque renouvellement et incident

Questions fréquentes

Nos fournisseurs sont plus gros que nous. Comment leur imposer quoi que ce soit ?

Aux géants (Microsoft, Google, grands SaaS), vous n'imposez rien — mais eux publient certifications, DPA et engagements : votre travail est de les lire et d'en garder trace. Le levier réel s'exerce sur les fournisseurs à votre échelle — prestataire IT, agence, éditeur local — précisément ceux dont la compromission vous frappe le plus fort. Et la question posée poliment déplace déjà le marché : les prestataires s'équipent parce que les clients demandent.

Un fournisseur critique refuse de répondre. On fait quoi ?

Graduer : reformuler en cinq questions simples (le questionnaire de 40 pages effraie légitimement), proposer l'alternative de la certification ou d'une attestation de son propre prestataire IT. Le refus persistant sur les basiques (MFA, notification d'incident) est une information en soi : compensez (accès réduits, sauvegardes, surveillance) et intégrez la sécurité aux critères du prochain appel d'offres. Documentez la démarche — c'est votre diligence en cas d'incident.

Sommes-nous responsables si notre fournisseur fuite nos données clients ?

Au sens RGPD : le responsable de traitement (vous) répond du choix et de l'encadrement de ses sous-traitants — d'où l'importance du DPA et de la diligence documentée ; le sous-traitant fautif engage aussi sa propre responsabilité. En pratique, une PME qui démontre avoir choisi sérieusement, contractualisé et réagi correctement est bien mieux positionnée — devant la CNIL comme devant ses clients.

Pour aller plus loin

ANSSI — maîtriser les risques de la sous-traitance — cyber.gouv.fr/publications/maitriser-les-risques-de-linfogerance

CNIL — le sous-traitant et l'article 28 — www.cnil.fr/fr/sous-traitance-queelles-sont-les-obligations

Structurer sans vous noyer dans la paperasse ?

Audit, mise en conformité, chartes et sensibilisation des équipes : un accompagnement à la taille de votre entreprise.

contact@cyberionis.fr · 06 64 90 07 74 · cyberionis.fr